Pavel Năstase
(coordonator)

Victoria Stanciu
Floarea Năstase
Mirela Gheorghe
Dana Boldeanu
Ali Eden
Gheorghe Popescu
Delia Băbeanu
Alexandru Gavrilă

AUDITUL ȘI CONTROLUL SISTEMELOR INFORMAȚIONALE



Cuprins

Preface

In the globally competitive business world of the 21st century, a well-controlled and effective corporate information system is a critical success factor for nearly every business organization. These organizational information systems must be monitored through well-defined information technology governance activities which include both effective information systems controls and information systems audit procedures.

Manipulation and abuse of accounting systems in conjunction with corporate frauds and financial statement misrepresentations have led to business failures or near bankruptcy situations at corporations around the world. These occurrences would include the well-publicized problems of Enron, World Com and others within the United States, as well as Parmalat and others in Europe. National governments have responded to these issues by developing more formal regulatory guidelines that demand stronger governance procedures within corporations and a more thorough review of these procedures by the external auditors that provide the opinions on the financial statements of these corporations. In the United States of America the highly consequential *Sarbanes-Oxley Public Company Accounting Reform and Investor Protection Act* (SOX) was passed in July 2002. Although this legislation only officially applies to companies that participate in the USA markets for capital and that are registered with the US Securities and Exchange Commission, the impact of the legislation has been felt around the world. Many countries already have enacted or are considering the enactment of similar legislation to strengthen the corporate governance activities in their countries. These acts have resulted in immediate and substantial changes in corporate governance activities and have had a significant impact over general and information systems audit controls and procedures.

Beyond the regulatory requirements, there are other developments that are increasing the importance of information technology governance for organizations. The capital investments that are required for state-of-the-art information systems in today's environment must lead directors and management teams to provide an increased emphasis on stewardship of these assets. As corporate organizations increase their overall governance activities they are necessarily increasing their attention upon information technology governance issues at the same time.

From the early stages of information systems development, there has been one global organization that has been dedicated to providing education, services, and leadership in the information technology area. ISACA® (formerly known as The Information Systems Audit and Control Association), was founded in 1969 and now has a membership of over 65,000 worldwide and its members live and work in more than 140 different countries. Today it is the global leader in information systems governance, security and controls. Its standards for information systems audit and controls are accepted by practitioners around the world and its Certified Information Systems Auditor® (CISA®) certification is recognize globally and has been earned by more that 50,000 professionals.

In 2004, ISACA released its *ISACA Model Curriculum for IS Audit and Control.* This document was developed to provide educators around the world with a basic framework of the educational topics and issues required to be taught to prepare students for entry level positons in the IS audit and control profession. The ISACA Model describes a comprehensive set of knowledge requirements that are much too substantial to be addressed in one textbook. However, this textbook is based upon the principles and guidelines established by the Model and it presents information about many of the most

important topics that must be mastered by students prior to entering the IS control profession. In addition, the book is based on many of the references that are recommended for preparing for the CISA certification examination. It reflects the authors' extensive theoretical and practical experiences in Romania in the professional fields of management information systems and auditing. The experiences of these authors not only include professional accounting, auditing, consulting, and information systems positions at a variety of banks and corporate organizations, but they also include many years of educational experience working with students at the Academy of Economic Studies of Bucharest.

The organizational structure and content of this text allow it to serve as a reference primer for studying the information systems audit and control discipline. At the end of each chapter there is a table or grid that readers can utilize to determine their level of knowledge in the chapter's topics. This grid assists the readers, whether they are students or professionals, to evaluate their insight about the concepts and assists them in the learning process. This text will be a valuable resource for educators who serve on Accounting and/or Management Information Systems Faculty groups. Students who are pursuing graduate programs at the master degree level will particularly benefit from this text. In addition, professionals and students will both want to refer to this work if they are looking for a resource to serve as a reference primer for future CISA certification exams. Practicing auditors will want to have this text as a part of their professional library because it will provide current knowledge about many information systems auditing and control topics. As you can see, this text will be valuable to all who wish to increase their knowledge base in this area.

The authors should be commended for their initiative and extensive efforts to develop and introduce such a high quality text in this area. The insight by the authors to base the structure of the book upon the ISACA Model curriculum should insure attention to the major topics required for students that wish to enter the IS auditor profession. Although this is only one text and it can not cover in sufficient detail all of the topics within the ISACA Model Curriculum, universities that adopt this text for their programs will be providing their students with excellent coverage of the most important topics. Eventually, usage of this text may lead to universities in Romania (like the Academy of Economic Studies of Bucharest) joining the list of internationally recognized schools that have entire programs that are in alignment with the ISACA Model Curriculum.

As the Chair of the global task force from ISACA that developed and wrote the 2004 *ISACA Model Curriculum for IS Audit and Control*, I think the authors have done a commendable job with this text. Their efforts should be well received by their faculty colleagues in Romania and the many students that will certainly benefit from their efforts as they use this text. Their efforts are welcomed by the profession and I want to express my congratulations on a job well done!

August 2007

Alan T. Lord

Dr. Alan T. Lord, CPA, CISA
Ernst & Young Professor of Accounting
Bowling Green State University
Bowling Green, Ohio USA

Cuvânt introductiv

Într-o economie globală şi bazată pe cunoştinţe, în care informaţia reprezintă al doilea factor important după resursele umane, auditul şi controlul sistemelor informaţionale devine din ce în ce mai important, ca urmare a impactului competitiv pe care îl are tehnologia informaţiei asupra mediului de afaceri.

Scandalurile din companiile americane Enron şi World Com au avut ca rezultat în ultimii ani o serie de schimbări în guvernanţa corporativă, cu un impact puternic asupra auditului şi controlului Sistemelor Informaţionale (SI). În luna iulie 2002, ca urmare a acestor evenimente, în SUA a fost adoptată *Legea reformei contabilităţii companiilor publice şi a protecţiei investitorilor* (*Sarbanes-Oxley Public Company Accounting Reform and Investor Protection Act* – SOX), care a direcţionat atenţia asupra auditului SI şi a rolului pe care acesta îl are în asigurarea acurateţei situaţiilor financiare şi a opiniei auditorilor financiari.

În Europa, Comitetul Basle II pentru supraveghere bancară recomandă o serie de condiţii care trebuie îndeplinite privind managementul riscului de credit, al celui operaţional, precum şi managementul sistemelor informaţionale. Un alt aspect care trebuie luat în considerare este creşterea continuă a investiţiilor în domeniul IT, ceea ce face ca managerii companiilor să fie foarte preocupaţi dacă aceste investiţii adaugă valoare la activitatea de bază pe care acestea o desfăşoară. Guvernanţa IT cere ca obiectivele IT să fie subordonate obiectivelor generale ale guvernanţei corporative a companiei.

Încă din perioada de început a sistemelor informatice, în anul 1969, a luat fiinţă *Asociaţia pentru Auditul şi Controlul Sistemelor Informaţionale (Information Systems Audit and Control Association – ISACA)*, care astăzi a devenit principala organizaţie în domeniul guvernanţei IT, securităţii şi controlului sistemelor informaţionale. Standardele pentru auditul şi controlul SI emise de ISACA sunt acceptate de toţi practicienii din domeniu, iar certificarea auditorilor de sisteme informaţionale *(Certified Information Systems Auditor – CISA)* este recunoscută la nivel internaţional, numărând astăzi peste 50.000 de profesionişti.

Obiectivul principal al acestei cărţi este de a oferi o viziune globală asupra auditului şi controlului sistemelor informaţionale, prezentând principalele tehnici şi metode, şi analizând câteva domenii importante ale SI.

Cartea este structurată în şapte capitole, după modelul de curiculă din 2004, oferită de departamentul de educaţie al ISACA, şi se bazează în principal pe tematica pentru pregătirea examenului de certificare CISA. Prezentarea la sfârşitul fiecărui capitol a unui test de tip grilă, pentru autoevaluarea cunoştinţelor, permite o înţelegere mai uşoară a conceptelor şi o apreciere graduală privind nivelul de pregătire a studenţilor.

Cartea reflectă experienţa pe care autorii o au în domeniul informaticii de gestiune, precum şi în practica de audit din România. O parte dintre autori sunt membrii ISACA, experţi contabili, auditori financiari şi, pe lângă activitatea didactică la ASE, desfăşoară şi activitate practică de consultanţă şi audit la diverse companii sau bănci.

Prin structura şi conţinutul său, cartea constituie un manual de referinţă pentru studiul disciplinei „Auditul şi controlul sistemelor informaţionale", care se predă în cadrul programelor de master la Facultatea de Contabilitate şi Informatică de Gestiune (CIG), precum şi la alte facultăţi cu profil economic din ţară. De asemenea, poate fi folosită ca un manual de pregătire în vederea examinării pentru certificarea CISA, precum şi de practicienii din domeniul auditului, pentru însuşirea cunoştinţelor necesare şi fundamentarea opiniilor acestora. Nu în ultimul rând, cartea se adresează tuturor celor care vor să se iniţieze în profesia de auditor IT.

Iniţiativa autorilor de a introduce în planul de învăţământ disciplina „Auditul şi controlul sistemelor informaţionale" şi de a scrie o carte cu acest titlu se încadrează în strategia ISACA, care prin departamentul de educaţie îşi propune să permită accesul studenţilor la profesia de auditor SI. În felul acesta, Facultatea de Contabilitate şi Informatică de Gestiune intră într-o reţea de universităţi care predau această disciplină în cadrul unor programe de master specializate pe sisteme informaţionale, din care fac parte trei universităţi din SUA: Bowling Green State University; University of Mississippi, California State University şi altele din Canada, Marea Britanie, Spania, Argentina, Olanda şi Hong Kong.

În elaborarea lucrării au fost consultate în principal referinţele bibliografice oferite de ISACA pentru pregătirea examenului de certificare CISA şi în mod special manualul „CISA Review Manual 2006". Autorii mulţumesc ISACA International şi Reprezentanţei ISACA din România pentru acordul dat privind utilizarea acestor referinţe bibliografice, precum şi pentru sprijinul şi încurajările oferite pe tot parcursul elaborării lucrării.

Cartea este prefaţată de profesorul Alan T. Lord de la Bowling Green State University din Ohio, SUA, care este preşedintele Comitetului ISACA pentru elaborarea programului de pregătire în domeniul auditului SI, fiind totodată un profesionist recunoscut în SUA (profesor de contabilitate la Ernst & Young, certificare CISA, CPA – *Certified Public Accountant).* Autorii mulţumesc profesorului Alan T. Lord pentru observaţiile şi sugestiile privind conţinutul cărţii, oferite cu ocazia participării sale în România la cea de-a doua Conferinţă Internaţională *Accounting and Management Information Systems (AMIS 2007)*, organizată de Facultatea de Contabilitate şi Informatică de Gestiune.

Lucrarea a fost elaborată în cadrul Catedrei de Informatică de Gestiune de la Academia de Studii Economice din Bucureşti, care a promovat disciplina „Auditul şi controlul sistemelor informaţionale" în planul de învăţământ al programelor de master, iar autorii mulţumesc cu acest prilej colegilor de catedră pentru observaţiile şi sugestiile competente, care au contribuit la realizarea acesteia.

Autorii mulţumesc de asemenea Editurii ECONOMICE pentru sprijinul acordat în publicarea cărţii.

August 2007 *Autorii*

Capitolul 1

Bazele teoretice şi conceptuale ale auditului sistemelor informaţionale

Capitolul 1

Bazele teoretice şi conceptuale ale auditului sistemelor informaţionale

1.1. Fundamentele teoretice ale auditului sistemelor informaţionale

În sens etimologic, cuvântul „audit" îşi are originea în latinescul „audire", care înseamnă „a asculta, a audia". Acest termen şi-a extins, în timp, aria semantică preluând sensuri precum „a examina, a verifica, a revizui conturi".

În literatura de specialitate, dar şi în practică, nu există un punct de vedere comun în ceea ce priveşte definirea conceptului de audit. Definiţia cel mai des invocată este însă cea prezentată în 1973 de Asociaţia Americană de Contabilitate (*American Accounting Association - AAA*) în cadrul „Declaraţiei privind conceptele de bază ale auditului". În această declaraţie se precizează că „auditul este un proces sistematic de obţinere şi evaluare obiectivă a unor afirmaţii privind acţiunile şi evenimentele cu caracter economic, în vederea aprecierii gradului de conformitate a acestor afirmaţii cu criteriile prestabilite, precum şi de comunicare a rezultatelor către utilizatorii interesaţi"[1].

Plecând de la acest cadru general, astăzi se observă că noţiunea de audit a fost asociată unor domenii diferite precum: auditul financiar, auditul mediului, auditul sistemelor informaţionale, auditul calităţii, auditul capitalului intelectual etc.

Informatizarea, ca efect al dezvoltării şi utilizării efective a tehnologiei informaţiei în diferite domenii, este o evoluţie normală şi o realitate ce a avut un impact deosebit şi asupra procesului de audit. Nevoia de adaptare a auditului la noile realităţi tehnologice, ţinând cont atât de avantajele generate de aceste tehnologii, cât şi de riscurile specifice mediilor informatizate, a avut un dublu impact: tehnologia informaţiei devine atât subiect, cât şi obiect al auditării. Altfel spus, pe de o parte, tehnologia informaţiei devine o resursă-cheie a oricărei organizaţii, care trebuie controlată şi auditată prin tehnici şi proceduri specifice, fapt ce a condus la apariţia auditului sistemelor informaţionale, iar pe de altă parte orice audit trebuie să integreze tehnologia informaţiei, iar adoptarea tehnicilor automate de audit reprezintă o cerinţă

---

[1] Declaraţia (*A Statement of Basic Auditing Concepts*) este analizată de V.M. O'Reilly, M.B. Hirsch, P.L. Defiliese, H.R. Jaenicke, în lucrarea *Mongomery's auditing*, Editura John Wiley & Sons, New York, ediţia a noua,1990.

generală într-un mediu în care sistemele auditate sunt informatizate pe o scară din ce în ce mai largă.

Integrarea tehnologiilor informatice în cadrul activităţilor economice ale unei organizaţii a condus la creşterea rolului sistemului informatic în prelucrarea datelor şi obţinerea informaţiilor economice. La început, această dependenţă tot mai crescută a afacerilor de tehnologiile informatice a solicitat auditorilor financiari nevoia de a se familiariza cu conceptele de prelucrare automată a datelor. Astfel în 1968, Institutul American al Contabililor Autorizaţi (*American Institute of Certified Public Accountants - AICPA*) a iniţiat dezvoltarea conceptului de ***auditul sistemelor de procesare automată a datelor*** (*Electronic Data Processing - EDP audit*). Auditorii financiari şi interni au realizat că sistemul informatic are un impact deosebit asupra obiectivelor misiunilor lor. Verificarea integrităţii datelor devine o etapă premergătoare îndeplinirii obiectivelor unei misiuni de audit financiar, deoarece auditorii trebuie să se asigure că rezultatele din rapoartele finale sunt bazate pe date complete, precise şi fiabile.

Nevoia unei organizaţii care să elaboreze standarde, ghiduri şi proceduri pentru auditul EDP s-a materializat în 1969, prin înfiinţarea Asociaţiei Auditorilor EDP (*Electronic Data Processing Auditors Association - EDPAA*).

Dezvoltarea accelerată a mediului e-business, utilizarea pe scară tot mai largă a resurselor disponibile pe *internet* a atras incidenţa unor riscuri informatice specifice, respectiv riscurile utilizării sistemelor informatice în prelucrarea şi transmisia datelor la distanţă. Fraudele şi pierderile de date în aceste sisteme se situează la un nivel ce nu poate fi ignorat, fapt ce a impus dezvoltarea în cadrul fiecărei organizaţii a unui *control intern orientat şi spre sistemul informatic*.

În mod natural, managerii s-au aflat în faţa unei noi provocări: *garantarea corectitudinii şi securităţii operaţiunilor din sistemul informatic.* Utilizarea explozivă a sistemelor informatice a dus inevitabil la evaluarea „încrederii" datelor prelucrate altfel decât cu tradiţionalele creion şi hârtie. O ipoteză tipică, mult folosită în realitatea practică, este aceea că informaţiile generate de calculator sunt întotdeauna corecte. În fapt, calculatorul nu face decât ceea ce este programat să facă şi, fără o testare prealabilă a mecanismelor de control din mediul informatizat, nu se poate concluziona că informaţiile produse de sistemul informatic sunt fiabile. Procedurile de control şi certificare a integrităţii datelor s-au născut din această nevoie de încredere.

În 1994, asociaţia EDPAA devine Asociaţia pentru Auditul şi Controlul Sistemelor Informaţionale (*Information Systems Audit and Control Association - ISACA*), recunoscută drept unica organizaţie profesională ce grupează şi certifică specialişti în domeniul auditului sistemelor informaţionale.

Astăzi, putem spune că necesitatea unui audit al sistemelor informaţionale au resimţit-o mai întâi auditorii financiari şi interni, privind-o la început doar ca pe o extensie a unui audit financiar, apoi managerii organizaţiilor, care, pentru a rezista în cursa concurenţiala creată, au recunoscut că tehnologia informaţiei reprezintă o resursă-cheie şi prin urmare trebuie controlate şi auditate procesele în care este utilizată şi, nu în ultimul rând, asociaţiile şi organizaţiile profesionale internaţionale au recunoscut necesitatea controlului şi auditarea sistemelor informatice.

Acest val al schimbărilor a avut efect şi asupra denumirii activităţii, ea evoluând de la auditul sistemelor de procesare automată a datelor (audit EDP) la auditul sistemelor informaţionale sau auditul sistemelor informatice (audit SI). Diferenţa conceptuală dintre aceşti termeni este dată, pe de o parte, de conţinutul şi nivelul la care se desfăşoară activitatea de audit şi, pe de altă parte, de diferenţa conceptuală care există între noţiunile de sistem informaţional şi sistem informatic. Astfel, auditul sistemului informaţional este cel mai cuprinzător, acoperind prin obiectivele sale toate nivelurile sistemului informaţional, de la evaluarea proiectării şi utilizării sistemului informatic, până la evaluarea politicilor şi procedurilor de securitate de la nivelul operaţional şi strategic. Auditul sistemului informatic, respectiv auditul informatic, acoperă prin obiectivele sale doar sistemul informatic. Concluzionând, auditul sistemului informaţional include auditul sistemului informatic.

În viziunea ISACA „auditul sistemelor informaţionale presupune verificarea şi evaluarea tuturor aspectelor legate de sistemele de prelucrare automată a datelor, incluzând şi prelucrările manuale care au legătură cu sistemul şi interfeţele între cele două sisteme." În literatura de specialitate, Ron Weber îl defineşte ca fiind „procesul prin care se colectează şi evaluează probe cu scopul de a determina dacă sistemul informaţional şi resursele implicate sunt protejate corespunzător, menţin integritatea datelor, oferă informaţii relevante şi contribuie la atingerea obiectivelor organizaţiei".

***Auditul sistemelor informaţionale** reprezintă o activitatea complexă de evaluare a unui sistem informatic în scopul emiterii unei opinii calificate asupra gradului de conformitate a sistemului cu standardele în domeniu şi, totodată, asupra capacităţii sistemului informatic de a atinge obiectivele strategice ale unei organizaţii, utilizând eficient resursele informaţionale şi asigurând integritatea datelor prelucrate şi stocate.*

De regulă, o astfel de activitate trebuie desfăşurată de o persoana competentă, cu o pregătire şi calificare în domeniul controlului, securităţii şi managementul sistemelor informaţionale (auditor SI). O atestare de acest gen este oferită de ISACA, prin certificatul CISA (*Certified Information Systems Auditor*).

Auditul SI poate fi realizat la nivelul oricărei organizaţii, regăsindu-se ca o componentă a auditului intern, dar poate fi realizat şi sub forma unui audit extern, atunci când managementul unei organizaţii solicită acest lucru.

Într-un cadru general, în funcţie de obiectivul propriu-zis al misiunii, auditorii sistemelor informaţionale urmăresc:

- *identificarea şi evaluarea riscurilor din sistem*;
- *verificarea separării funcţiilor incompatibile în cadrul sistemului informatic;*
- *verificarea securităţii fizice şi logice a sistemului informaţional*;
- *verificarea şi evaluarea infrastructurii reţelelor de calculatoare*;
- *controlul aplicaţiilor informatice existente în sistem*;
- *testarea integrităţii datelor*;
- *verificarea existenţei şi securităţii copiilor de siguranţă a datelor, informaţiilor, aplicaţiilor informatice;*
- *verificarea şi evaluarea planurilor de recuperare în caz de dezastre.*

În prezent, în România, activitatea de audit a sistemelor informaţionale nu este bine delimitată, ea regăsindu-se, pe de o parte, ca o subactivitate a auditului financiar şi a auditului intern, iar pe de altă parte, ca o cerinţă impusă prin *Regulamentul BNR nr. 4/2002*, privind tranzacţiile efectuate prin intermediul instrumentelor de plată electronică şi relaţiile dintre participanţii la aceste tranzacţii.

Ca o concluzie, putem sublinia faptul că, astăzi, într-un mediu puternic informatizat, activitatea de audit al sistemelor informaţionale a devenit o necesitate stringentă, iar efectele unei astfel de misiuni se pot concretiza în creşterea securităţii mijloacelor sistemului informaţional, asigurarea integrităţii datelor, creşterea eficienţei exploatării sistemului informaţional şi de asemenea creşterea calităţii controlului intern.

1.2. Standarde şi ghiduri pentru auditul sistemelor informaţionale

Pe plan internaţional, în domeniul auditului sistemelor informaţionale, cea mai cunoscută autoritate este ISACA, asociaţie care a elaborat standardele de audit al sistemelor informaţionale şi care are astăzi 170 de filiale în peste 70 de ţări, numărând peste 50.000 de membri.

Ca prim element iniţiat de ISACA a fost elaborarea unui **Cod de etică profesională** pentru auditori. Acesta reprezintă un set de reguli de comportament, care ghidează conduita etică şi profesională a membrilor săi, cât şi a auditorilor certificaţi.

Principiile etice profesionale fundamentale stipulate în acest cod solicită membrilor ISACA şi auditorilor următoarele:

- să susţină implementarea standardelor, procedurilor de auditare a sistemelor informaţionale;
- să servească interesul clienţilor săi cu loialitate, seriozitate şi să nu participe cu bună ştiinţă la activităţi ilegale;
- să păstreze confidenţialitatea informaţiilor obţinute în timpul misiunilor efectuate, exceptând situaţiile în care dezvăluirea acestora este solicitată de o autoritate legală;
- să aibă o atitudine independentă care-i va permite să acţioneze în mod corect şi fără prejudecăţi;
- să dea dovadă de profesionalism şi să nu accepte nicio misiune dacă nu are cunoştinţele, aptitudinile sau resursele necesare de a realiza lucrările unei astfel de acţiuni. Ei trebuie să-şi asume responsabilitatea opiniei şi a recomandărilor pe care le exprimă în raportul de audit;
- să informeze părţile implicate despre rezultatele auditului, dezvăluind toate aspectele semnificative pe care le-au sesizat;
- să susţină informarea acţionarilor, pentru a creşte înţelegerea lor în ceea ce priveşte securitatea şi controlul sistemelor informaţionale.

Codul de etică profesională a constituit o primă provocare pentru această organizaţie, ea fiind urmată de elaborarea **Standardelor internaţionale de audit a sistemelor informaţionale** care au permis uniformizarea internaţională a practicilor de audit. Obiectivul acestor standarde este de a oferi, pe de o parte, auditorului un set de reguli şi principii la care se poate raporta în timpul exercitării misiunii sale, iar pe de altă parte, de a informa conducerea organizaţiei şi pe cei interesaţi cu privire la modul de desfăşurare a activităţilor şi practicile specifice acestui domeniu.

În mod practic, pentru a sprijini implementarea cu succes a standardelor, ISACA a publicat o serie de ***ghiduri metodologice*** – care îi oferă auditorului elementele practice de aplicare a standardelor de audit, cât şi un set de ***proceduri*** – reprezentate printr-o colecţie de exemple de proceduri pe care un auditor trebuie să le urmeze într-o misiune de audit a sistemelor informaţionale.

Standardele internaţionale de audit pentru sistemele informaţionale sunt:
S1. Contractul de audit (*Audit Charter*). În viziunea acestui standard, scopul, responsabilitatea şi autoritatea funcţiei de audit a sistemelor informaţionale trebuie sa fie în mod clar stipulate printr-un contract de audit sau o scrisoare de angajament.
S2. Independenţa (*Independence*). Independenţa, în general, este „piatra de încercare" a profesiei de auditor. Standardul vizează două aspecte de bază:

- *independenţa profesională*: pe parcursul misiunii sale, auditorul sistemelor informaţionale trebuie să fie independent în comportament faţă de organizaţia auditată, indiferent de atitudinea acesteia sau situaţiile întâlnite;

- *independența organizațională*: funcția de audit a sistemelor informaționale trebuie să fie independentă față de aria auditată, pentru a permite auditorului atingerea în totalitate a obiectivelor sale.

S3. Etica şi standardele profesionale (*Professional Ethics and Standards*) care vizează două aspecte:

- auditorul SI trebuie să respecte Codul etic profesional emis de ISACA;
- auditorul SI trebuie să-şi exercite profesia respectând standardele profesionale de audit aflate în vigoare, la momentul desfăşurării misiunii.

S4. Competența profesională (*Professional Competence*). Prezentul standard cuprinde două elemente definitorii:

- auditorul SI trebuie să fie competent din punct de vedere profesional, având *aptitudinile şi cunoştințele necesare* pentru a conduce misiunea de audit;
- auditorul trebuie să-şi mențină competența profesională printr-o *formare şi educare continue*.

S5. Planificarea (*Planning*):

- auditorul SI trebuie să planifice activitatea de audit în funcție de obiectivele misiunii sale şi în concordanță cu legile şi standardele de audit aflate în vigoare;
- auditorul SI trebuie să dezvolte şi să elaboreze o strategie de audit bazată pe riscuri;
- auditorul SI trebuie să elaboreze şi să documenteze un plan de audit care să stabilească natura şi obiectivele, durata şi întinderea misiunii de audit, cât şi resursele necesare.

S6. Performanța activității de audit (*Performance of Audit Work*):

- supervizare – conducătorul misiunii de audit îşi va supraveghea echipa de specialişti pentru a se asigura de atingerea obiectivelor propuse şi respectarea standardelor de audit;
- probele de audit – pe parcursul misiunii sale, auditorul SI trebuie să obțină probe suficiente, relevante şi de încredere pentru a-şi îndeplini obiectivele de audit. Concluziile finale trebuie să se bazeze pe analiza şi interpretarea acestor probe de audit;
- documentarea – procesul de audit trebuie să fie documentat, auditorul descriind în foile sale de lucru munca de audit desfăşurată, probele care susțin concluziile sale finale.

S7. Raportarea (*Reporting*):

- la sfârşitul misiunii de audit, auditorul SI va furniza un raport care trebuie să identifice organizația auditată, destinatarii raportului şi eventuale restricții de circulație a acestuia;
- raportul de audit reprezintă instrumentul prin care se comunică scopul auditării, obiectivele urmărite, perioada acoperită, natura şi întinderea procedurilor de audit. În cuprinsul său se regăsesc, de asemenea, constatările

şi concluziile misiunii, precum şi orice rezervă pe care auditorul o are asupra sistemului auditat;

- raportul de audit trebuie să fie semnat şi realizat în termenul stabilit prin contractul de audit sau scrisoarea de angajament.

S8. Urmărirea recomandărilor raportului de audit (*Follow-up Activities*): După raportarea concluziilor şi a recomandărilor făcute, auditorul SI trebuie să revină şi să evalueze măsurile luate de managementul organizaţiei pentru realizarea recomandărilor sale.

S9. Frauda şi eroarea (*Irregularities and Illegal Acts*):

- în planificarea şi desfăşurarea activităţii de audit, pentru a reduce riscul de audit la un nivel acceptabil, auditorul SI trebuie să evalueze riscul apariţiei unor fraude şi/sau erori;
- auditorul SI trebuie să-şi menţină o atitudine profesională de scepticism pe durata misiunii sale, ţinând cont de posibilitatea existenţei unor acte ilegale.

S10. Guvernanţa IT (*IT Governance*). În viziunea acestui standard, auditorul SI trebuie:

- să analizeze şi evalueze dacă sistemul informaţional al organizaţiei susţine obiectivele şi strategiile acesteia;
- să evalueze eficienţa utilizării resurselor sistemului informaţional şi performanţa proceselor manageriale IT;
- să analizeze managementul riscurilor asociate tehnologiilor informatice.

S11. Utilizarea evaluării riscului în planificarea auditului (*Use of Risk Assesment in Audit Planning*). În planificarea misiunii de audit şi stabilirea priorităţilor pentru o alocare efectivă a resurselor de audit, auditorul SI trebuie să utilizeze o evaluare bazată pe riscuri. Această abordare îl va determina pe auditor să-şi concentreze atenţia asupra punctelor sensibile ale sistemului auditat, fără a se pierde în detalii inutile.

S12. Pragul de semnificaţie în audit (*Audit Materiality*):

- auditorul SI trebuie să ia în considere pragul de semnificaţie şi relaţia acestuia cu riscul de audit pentru a determina natura, durata şi întinderea procedurilor de audit;
- există o relaţie inversă între pragul de semnificaţie şi nivelul riscului de audit, şi anume, cu cât este mai înalt pragul de semnificaţie cu atât este mai scăzut riscul de audit şi invers.

S13. Utilizarea informaţiilor obţinute de la alţi experţi (*Using the Work of Other Experts*):

- auditorul SI trebuie, acolo unde este cazul, să folosească experienţa şi expertiza unor experţi;
- un expert poate fi un auditor SI din exteriorul firmei de audit, un consultant managerial, un expert IT etc.;
- atunci când optează pentru utilizarea unui expert, auditorul trebuie să evalueze competenţa profesională, experienţa şi independenţa acestuia;

- auditorul trebuie să obţină suficiente probe de audit adecvate privind faptul că aria de aplicabilitate a serviciilor expertului corespund scopurilor auditului.

S14. Probele de audit (*Audit Evidence*):

- auditorul trebuie să obţină probe de audit suficiente şi relevante pentru a fi capabil să emită concluzii rezonabile pe care să se bazeze opinia de audit;
- auditorul trebuie să evalueze suficienţa probelor obţinute pe parcursul misiunii.

Pe plan naţional, se simte nevoia unui cadru normativ şi legal pentru domeniul auditului sistemelor informaţionale. În ultimii ani, au apărut din ce în ce mai multe reglementări legislative privind protecţia şi securitatea informaţiilor, cum ar fi:

- *Legea nr. 365/2002* privind comerţul electronic;
- *Legea nr. 455/2001* privind semnătura electronică;
- *Legea nr. 506/2004* privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice;
- *Legea nr. 102/2005* privind înfiinţarea, organizarea şi funcţionarea *Autorităţii Naţionale de Supraveghere* a Prelucrării Datelor cu Caracter Personal;
- *Legea nr. 64/2004* pentru ratificarea *Convenţiei Consiliului Europei* privind criminalitatea informatică.

De asemenea, se impun a fi amintite şi standardele adoptate în România, standarde care vizează aspecte legate de asigurarea securităţii informaţionale:

- **ISO/IEC 27001:2005** *„Tehnologia informaţiei – Tehnici de securitate – Sisteme de management al informaţiilor – Cerinţe"* este un standard care stabileşte cerinţele pentru un sistem de management al securităţii informaţiei. În fapt, el ajută la identificarea, managementul şi minimizarea ameninţărilor care afectează de obicei informaţia;
- **ISO/IEC 17799** *„Tehnologia Informaţiei - Cod de bună practică pentru managementul securităţii informaţiei"* reprezintă un ghid pentru implementarea unui set de politici, practici şi proceduri în vederea consolidării securităţii informaţiei gestionate de o organizaţie.

1.3. Planificarea şi managementul auditului sistemelor informaţionale

1.3.1. Cadrul general al unui proces de audit al sistemelor informaţionale

Definirea unei imagini de ansamblu asociată procesului de audit impune prezentarea succintă a fazelor de desfăşurare a acestei misiuni:

Faze de audit	Descrierea
1. Subiectul auditului	• Identifică aria ce va fi auditată
2. Obiectivul auditului	• Identifică obiectivul auditului, spre exemplu, un obiectiv poate fi reprezentat de analiza modificărilor programelor-sursă.
3. Scopul auditului	• Identifică sistemele specifice, funcţiile şi ariile ce vor fi verificate. Spre exemplu, pentru obiectivul expus mai sus, scopul declarat limitează verificarea la un singur sistem sau la o perioadă de timp.
4. Planificarea	• Identifică sursele de informaţii pentru testare sau evaluarea rezultatelor, precum diagramele funcţionale, politicile, standardele, procedurile unor misiuni de audit anterioare. • Identifică locaţiile sau resursele ce vor fi auditate. • Identifică resursele necesare pentru desfăşurarea misiunii.
5. Proceduri de audit pentru culegerea probelor	• Identifică şi selectează abordarea auditului pentru verificarea şi testarea controalelor. • Identifică personalul-cheie pentru intervievare. • Analizează politicile departamentelor, normele şi ghidurile interne. • Dezvoltă instrumente de audit şi metodologii de testare şi verificare a controlului.
6. Proceduri pentru evaluarea rezultatelor testării	• Specific organizaţiei

7. Proceduri de comunicare cu managementul	• Specific organizaţiei
8. Pregătirea raportului de audit	• Identifică recomandările necesare. • Identifică procedurile de evaluare/testare a eficienţei operaţionale.

1.3.2. Planificarea auditului sistemelor informaţionale

Planificarea auditului este prima etapă a unui proces de audit, al cărui scop principal îl reprezintă asigurarea eficienţei şi execuţia efectivă a tuturor etapelor acestui proces. O planificare adecvată a activităţii de audit permite identificarea domeniilor semnificative de audit, a punctelor slabe din cadrul sistemului şi, totodată, este primul pas în realizarea unui audit eficient. Această acţiune va fi diferită în funcţie de mărimea organizaţiei, complexitatea auditului, experienţa auditorului şi, nu în ultimul rând, de cunoaşterea activităţilor desfăşurate în cadrul organizaţiei.

Planificarea activităţii de audit are ca scop definirea ariei de audit şi a modului de abordare a auditului, precizarea obiectivelor misiunii, stabilirea activităţilor, termenelor şi responsabilităţilor, a bugetului necesar îndeplinirii obiectivelor misiunii.

Pe parcursul acestei etape, auditorul SI trebuie să desfăşoare o serie de proceduri:

- să se informeze cu privire la obiectul de activitate al clientului şi domeniul în care îşi desfăşoară activitatea;
- să se documenteze cu privire la structura sistemului informaţional. Auditorul trebuie să analizeze structura organizatorică (organigrama), organigrama sistemului informatic şi diagramele din sistem; să se documenteze cu privire la politicile şi procedurile de securitate, respectiv procedurile de operare din sistemul informatic, să identifice contractele de externalizare din sistemul informaţional;
- să identifice politicile, standardele şi ghidurile necesare domeniului auditat;
- să analizeze riscurile;
- să evalueze controalele interne;
- să stabilească nivelul pragului de semnificaţie;
- să stabilească obiectivele auditului;
- să dezvolte o strategie de audit;
- să planifice resursele de personal necesare şi să le asocieze responsabilităţi concrete.

În cadrul etapei de planificare, ***activitatea de cunoaştere a clientului, înţelegerea sistemului informaţional*** reprezintă un element esenţial pentru bunul mers al

acţiunilor ce vor urma. Tehnicile şi metodele folosite de auditor pentru culegerea informaţiilor sunt:

- analiza planurilor strategice pe termen lung;
- consultarea unor publicaţii, rapoarte anuale şi analize financiare;
- interviuri cu managerii din poziţiile-cheie ale organizaţiei pentru a înţelege cerinţele afacerii;
- interviuri cu managementul IT şi persoanele implicate în administrarea, monitorizarea, întreţinerea şi utilizarea sistemului informatic;
- consultarea legislaţiei aferente domeniului auditat;
- consultarea rapoartelor misiunilor de audit anterioare.

Pe baza informaţiilor culese, auditorul va efectua o ***analiză a riscurilor***, în special a riscurilor inerente care decurg din natura activităţilor desfăşurate. Această analiză va permite identificarea ameninţărilor şi vulnerabilităţilor sistemului informaţional, fiind urmată de ***evaluarea controalelor interne*** existente în cadrul departamentelor şi sistemelor organizaţiei. Tot acest demers îi va permite auditorului formularea unui prediagnostic, stabilirea obiectivelor specifice de auditat, a „punctelor slabe" ce vor fi analizate în detaliu şi dezvoltarea unei strategii de audit.

Standardul de audit ISACA „S5. Planning" recomandă auditorilor să dezvolte şi să elaboreze o ***strategie de audit bazată pe riscuri***.

Finalitatea acestei etape o reprezintă elaborarea unui ***plan de audit*** care va stabili natura şi aria de întindere a lucrărilor ce urmează a fi desfăşurate, cât şi măsurile organizatorice necesare pentru executarea lor în condiţii de eficienţă maximă. Pe parcursul misiunii se admit ajustări ale planului de audit, cerute de apariţia unor noi elemente semnificative ce solicită investigaţii mai adânci, teste mai detaliate.

1.3.2.1. Analiza riscului

În ultimii ani, auditul SI a trecut de la o abordare orientată spre controlul sistemului la o abordare orientată spre riscurile la care acesta este expus. La această reorientare a concurat şi eşecul în prevenirea unor cazuri precum: ENRON, WorldCom, PARMALAT. Înţelegerea mediului de control, a caracteristicilor sistemului informaţional în ansamblul său, este un pas important şi hotărâtor pentru auditori, în vederea stabilirii gradului de credibilitate a sistemului însuşi şi a informaţiilor pe care le furnizează. Orientarea spre evaluarea riscurilor permite auditorului să observe mult mai bine eficacitatea şi eficienţa controlului din sistemul auditat.

Analiza riscului face parte din planificarea auditului şi permite identificarea riscurilor şi vulnerabilităţilor astfel încât auditorul să poată determina controalele necesare pentru a minimiza aceste riscuri.

În literatura de specialitate se regăsesc mai multe definiţii asociate conceptului de risc. Dominique Vincenti[2] defineşte riscul ca fiind „ameninţarea ca un eveniment sau o acţiune să aibă un impact defavorabil asupra capacităţii organizaţiei de a-şi îndeplini cu succes obiectivele".

O altă definiţie oferită de *Guidelines for the Management of IT Securities* (publicat de Organizaţia Internaţională pentru Standardizare) asociată conceptului de risc în mediul informatizat este „potenţialul ca o ameninţare dată va exploata vulnerabilităţile unui activ sau grup de active cauzând pierderea sau paguba activelor. Impactul este proporţional cu valoarea pierderii sau pagubei şi frecvenţa estimată a ameninţării."

În acest context, riscul poate fi caracterizat prin următoarele elemente:

- ameninţările, cât şi vulnerabilităţile asociate proceselor şi/sau activelor informaţionale;
- impactul ameninţărilor şi vulnerabilităţilor asupra activelor;
- probabilitatea de realizare a ameninţărilor (combinaţia dintre probabilitatea şi frecvenţa de apariţie).

Ameninţările sunt acele evenimente sau activităţi, în general externe unui sistem, care pot afecta la un moment dat punctele slabe (vulnerabilităţile) ale acestuia, cauzând pierderi semnificative. În general, o ameninţare este o forţă potenţială care poate afecta disponibilitatea, confidenţialitatea şi integritatea sistemului, generând adeseori întreruperi de servicii ale acestuia. În practică, se întâlnesc situaţii când o ameninţare poate exista într-un sistem o perioadă lungă de timp, fără a avea un impact asupra acestuia, în timp ce o alta poate avea un impact imediat după apariţia sa. De asemenea, probabilitatea de apariţie a unei ameninţări într-o perioadă de timp este mai mare decât a altora (spre exemplu, erorile cauzate de introducerea greşită a datelor de la tastatură sunt mai frecvente decât „căderile" sistemului).

Riscul la nivelul unei organizaţii nu poate fi eliminat, el va exista întotdeauna, managementul organizaţiei fiind responsabil de reducerea lui la un nivel acceptabil. În acest sens, figura 1.3.1 pune în corespondenţă diferite elemente ce necesită a fi analizate pentru reducerea riscului.

[2] Dominique Vincenti –„Dresser une cartographie des risques", în *Revista de Audit,* nr. 144, citată de Jacques Renard în *Teoria şi practica auditului intern.*

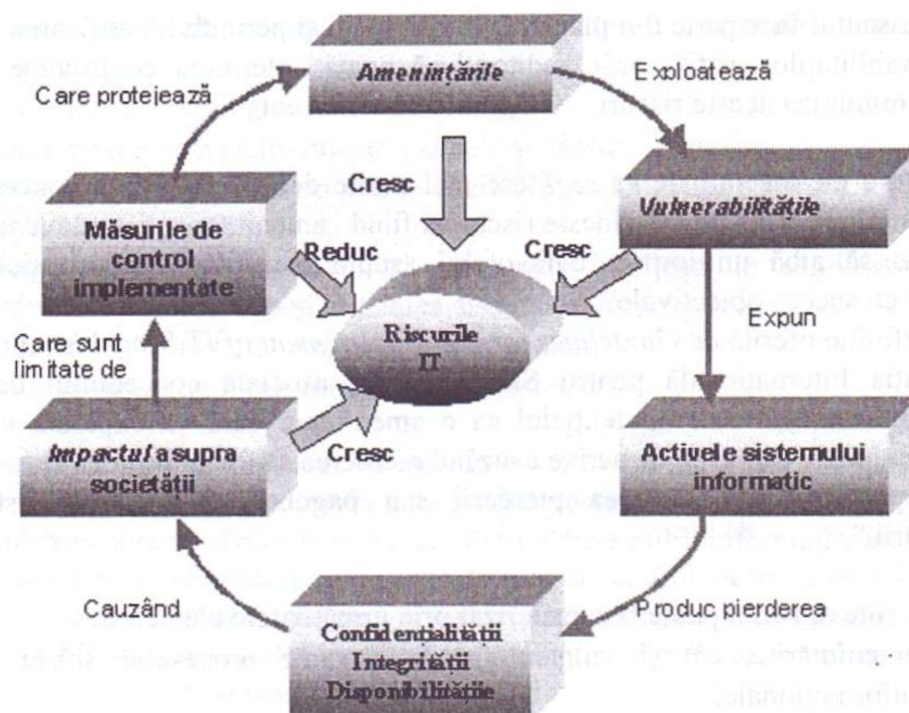


Figura 1.3.1. **Analiza riscului IT**[3]

Auditorul SI se va concentra asupra riscurilor semnificative care pot afecta confidenţialitatea, disponibilitatea şi integritatea informaţiilor critice dintr-un sistem. În cadrul acestui proces de analiză, auditorii SI vor evalua eficienţa procesului de management al riscurilor dintr-o organizaţie.

Literatura de specialitate defineşte **managementul riscului** ca fiind „procesul de identificare a vulnerabilităţilor şi ameninţărilor din cadrul unei organizaţii, precum şi de elaborare a unor măsuri de minimizare a impactului acestora asupra resurselor informaţionale". Procesul este caracterizat printr-un ciclu de viaţă interactiv care începe cu ***identificarea activelor*** ce se doresc a fi protejate (hardware, software, baze de date, reţele, informaţii, suporţi de memorare etc.). Odată ce activele informatice critice sunt identificate, este realizată ***evaluarea riscurilor***. Această etapă presupune mai întâi identificarea riscurilor asociate acestor active, apoi evaluarea lor în funcţie de gravitatea efectelor pe care le produc pentru a se determina impactul rezultant. A treia etapă, ***minimizarea riscurilor,*** implică o identificare a controalelor ce vor permite minimizarea riscurilor identificate. În general, aceste controale vor preveni sau reduce probabilitatea de apariţie a riscurilor, pot detecta un eveniment generator de risc, minimiza impactul sau transfera riscul către altă organizaţie (externalizare).

[3] Prelucrare după INTOSAI IT AUDIT COMMITTEE – IT Security, note de curs, www.intosai.com

Analiza şi evaluarea acestor măsuri de prevenire poate fi realizată prin analize cost-beneficiu care vor urmări:

- costul controlului comparativ cu beneficiul minimizării riscului;
- nivelul riscului rezidual (definit ca acel nivel de risc ce rămâne după analiza şi evaluarea tuturor măsurilor de combatere a riscurilor) pe care managementul este pregătit să-l accepte;
- metode de reducere a riscului preferate (eliminarea/evitarea, diminuarea frecvenţei de apariţie sau a impactului, transfer către alte organizaţii/asigurare).

Ultima etapă, ***reevaluarea riscului***, permite o monitorizare a performanţei nivelurilor de risc.

Aceste trei etape – evaluarea riscului, minimizarea şi reevaluarea acestuia – se desfăşoară cu scopul de a minimiza riscul la un nivel acceptabil de către management.

Analiza riscului, realizată în cadrul etapei de planificare, ajută auditorul SI în:

- identificarea riscurilor şi ameninţărilor mediului IT. În mod practic, această analiză oferă auditorului selectarea ariilor critice care vor fi supuse auditării;
- evaluarea asupra controalelor existente, încă din faza de planificare;
- determinarea obiectivelor specifice de auditare;
- susţinerea deciziei de audit bazată pe risc.

1.3.2.2. Controlul intern

Controlul intern la nivelul unei organizaţii poate fi definit ca un ansamblu de politici, proceduri, practici şi structuri organizaţionale implementate pentru a reduce riscurile. Acestea sunt dezvoltate pentru a oferi o asigurare rezonabilă că obiectivele organizaţiei vor fi îndeplinite urmărind prevenirea, detectarea şi corectarea evenimentelor care ar putea afecta într-un mod negativ organizaţia.

Astfel, controlul intern poate fi:

- *preventiv*: permite prevenirea producerii erorilor, omisiunilor şi acţiunilor rău-voitoare. De exemplu, în cadrul controlului preventiv din sistemul informaţional pot fi cuprinse următoarele acţiuni: angajarea personalului având o calificare în domeniu, separarea sarcinilor şi responsabilităţilor; controlul accesului fizic la resursele din sistem (pe bază de cartele sau carduri de acces); stabilirea unor proceduri de autorizare a tranzacţiilor, stabilirea unor proceduri clare de introducere a datelor în sistem, controlul accesului logic la resursele sistemului astfel încât numai persoane autorizate să aibă acces la informaţiile sensibile;
- *detectiv*: permite detectarea şi raportarea problemelor apărute în sistem. De exemplu, în cadrul controlului detectiv din sistemul informaţional pot fi

cuprinse: validarea intrărilor de date prin caractere de control; mesajele de eroare din cadrul aplicaţiilor informatice; procedura de identificare a înregistrărilor duplicate într-o bază de date, a controlului totalurilor loturilor prelucrate, funcţia de audit intern;
- *corectiv*: permite reducerea impactului unei ameninţări identificate prin controlul detectiv sau permite corectarea erorilor detectate. De exemplu, procedurile de recuperare a datelor; procedurile de relansare a aplicaţiilor informatice.

Activităţile de control intern pot fi realizate atât prin proceduri manuale, cât şi automate. Obiectivele controlului intern[4] specifice sistemului informaţional urmăresc:
- protejarea şi securitatea activelor organizaţiei;
- asigurarea integrităţii mediului de control;
- asigurarea integrităţii aplicaţiilor informatice existente în sistem prin:
  - autorizarea intrărilor de date;
  - acurateţea şi completitudinea procesării tranzacţiilor;
  - încrederea în activitatea de procesare a informaţiilor;
  - acurateţea, completitudinea şi încrederea rapoartelor;
  - integritatea bazelor de date;
- asigurarea eficienţei exploatării sistemului informatic;
- conformitatea cu cerinţele utilizatorilor, politicile şi procedurile organizaţiei, reglementările şi legile în vigoare;
- dezvoltarea planurilor de continuitate a activităţii şi recuperare a datelor în caz de dezastre;
- dezvoltarea unor planuri de acţiune în cazul evenimentelor neprevăzute.

Institutul de guvernanţă IT a publicat un cadru de lucru pentru controlul şi guvernanţa IT care înglobează cele mai bune practici pentru managementul IT - COBIT (*Control Objectives for Business & Related Technology*). Acesta este proiectat să constituie un ghid accesibil pentru management, utilizatori şi auditori asigurându-le confidenţialitatea, integritatea şi disponibilitatea datelor şi informaţiilor.

1.3.2.3. Pragul de semnificaţie şi riscul de audit

Practica a demonstrat, în general, că nu există timp suficient pentru a realiza un audit detaliat. Acesta este şi motivul pentru care auditorul acceptă încă de la începutul misiunii sale că va lucra cu o anumită marjă de eroare. El trebuie să stabilească însă care este mărimea erorii pe care o poate accepta, în cadrul fiecărei misiuni individuale. Dimensiunea marjei de eroare determină pragul de semnificaţie,

---
[4] Prelucrare după CISA 2005.

recunoscut ca o „graniță" de la care auditorul va trebui să detecteze eventualele anomalii semnificative, mărimea și natura acestora.

A evalua ce este esențial, semnificativ, este o problemă de judecată profesională și se analizează prin prisma efectului general al erorilor, omisiunilor, fraudelor și al altor ilegalități asupra organizației.

Alegerea pragului de semnificație, în cadrul unui audit SI, poate fi mult mai dificilă. Auditorul trebuie să considere atât aspectele cantitative, cât și pe cele calitative în stabilirea pragului de semnificație.

În acest sens, auditorul SI trebuie să considere:

- nivelul posibil al erorilor acceptat de management;
- potențialul efectelor cumulate al erorilor minime sau breșelor care pot avea un efect semnificativ.

În elaborarea planului de audit, auditorul impune un nivel acceptabil al pragului de semnificație, astfel încât să poată detecta, din punct de vedere cantitativ, informațiile eronate semnificativ.

Standardul de audit ISACA „S9. Audit Materiality" recomandă auditorilor SI să analizeze raportul invers proporțional care există între pragul de semnificație și riscul de audit pentru a determina natura, durata și întinderea procedurilor de audit. Pragul de semnificație, combinat cu riscul de audit, este considerat esențial pentru planificarea ariilor ce vor fi auditate.

Riscul de audit reprezintă probabilitatea ca un auditor să nu observe o eroare sau fraudă din sistemul auditat, formulând astfel o opinie greșită. El se manifestă prin componentele sale de bază: **risc inerent, risc de control și risc de nedetectare** și poate fi stabilit atât în termeni cantitativi (în procente), cât și în termeni calitativi (risc scăzut, moderat, ridicat sau foarte ridicat).

- *Riscul inerent* reprezintă probabilitatea ca o eroare sau o fraudă să se producă în mod inerent ca urmare a naturii activității desfășurate în cadrul organizației. Riscul inerent există independent de activitatea de audit și se manifestă datorită naturii activităților din cadrul organizației.
- *Riscul de control* reprezintă probabilitatea ca o eroare sau o fraudă să se producă fără a fi detectată sau prevenită în timp util de sistemul de control intern. De exemplu, riscul pe care îl implică verificarea manuală a jurnalelor dintr-un sistem informatic este considerat mare, datorită volumului semnificativ de informații înmagazinate în aceste jurnale. Pe de altă parte, riscul controlului asociat procedurilor automate de validare a datelor este considerat redus, datorită continuității acestui control și a testelor efectuate înainte de exploatarea aplicației.

Atât riscul inerent, cât şi riscul de control nu pot fi controlate de auditor, aceste riscuri există independent de activitatea de audit. Riscul inerent şi riscul de control sunt intercorelate, iar o evaluare separată a acestora poate conduce la o apreciere necorespunzătoare a riscului de audit.

- *Riscul de nedetectare* reprezintă probabilitatea ca un auditor să nu detecteze prin testele aplicate o eroare din cadrul sistemului de control auditat. Spre exemplu, riscul de nedetectare asociat identificării punctelor slabe ale securităţii sistemului va fi mare dacă jurnalele pentru întreaga perioadă supusă auditului nu vor fi disponibile în totalitate în momentul verificărilor. El este singurul risc controlat de auditor şi este direct legat de testele de fond pe care acesta le va aplica.
- *Riscul global* – combinaţia tuturor categoriilor de riscuri de audit evaluate pentru fiecare obiectiv specific de control.

Remarcă: Riscul de audit nu trebuie confundat cu riscul de eşantionare.

Obiectivul principal al auditorului este de a proiecta şi implementa proceduri de audit care să-i permită reducerea riscului de audit la un nivel acceptabil. Această evaluare, recunoscută de literatura de specialitate şi legislaţia în vigoare ca o etapă obligatorie în cadrul unei misiuni de audit, nu se realizează cu ajutorul unei metode unice.

1.3.2.4. Stabilirea obiectivelor auditului

În etapa de planificare a unei misiuni de audit, un aspect important îl reprezintă stabilirea obiectivelor misiunii. În general, obiectivele unui audit urmăresc să verifice dacă controalele interne existente minimizează riscurile unei organizaţii. Aceste obiective de audit urmăresc asigurarea conformităţii cu cerinţele legale şi de reglementare în vigoare, cât şi a confidenţialităţii, integrităţii, disponibilităţii şi încrederii resurselor informaţionale.

Stabilirea obiectivelor unui audit SI determină abordarea auditului şi influenţează întregul flux al activităţilor desfăşurate în cadrul acestuia. Stabilirea obiectivului general se face în funcţie de scopul evaluării care poate fi: evaluarea performanţei unei activităţi, evaluarea unei aplicaţii sau a unui sistem bazat pe tehnologia informaţiei, evaluarea tehnică a unui sistem sau a unei aplicaţii. Plecând de la aceasta premisă, se pot nuanţa diferite abordări ale unui audit SI:

1. evaluarea unui sistem informaţional integrat sau a unor aplicaţii utilizate în cadrul organizaţiei auditate;
2. evaluarea unui sistem informatic în scopul furnizării unei asigurări rezonabile asupra funcţionării acestuia, proces necesar, spre exemplu, în cadrul unei misiuni de audit financiar care se desfăşoară în cadrul organizaţiei;

3. evaluarea performanţei unei activităţi, a unui program sau a unui sistem informaţional.

După stabilirea obiectivului general, se formulează obiectivele specifice, care determină cerinţele şi criteriile concrete care vor sta la baza evaluării. La nivelul unui audit SI, cu titlu de exemplu, menţionăm câteva obiective specifice generice:

- evaluarea eficienţei sistemului;
- evaluarea soluţiilor de implementare şi de utilizare a sistemului informatic;
- asigurarea securităţii sistemului informatic;
- managementul continuităţii activităţii;
- identificarea şi evaluarea riscurilor IT;
- evaluarea proiectării şi dezvoltării unui sistem;
- formularea unor recomandări pentru perfecţionarea sistemului informatic.

1.4. Desfăşurarea procesului de audit al sistemelor informaţionale

Orice proces generic de audit, indiferent de obiectivul său, se va desfăşura şi va urmări procedurile generale de audit:

- obţinerea unei înţelegeri a ariei de auditat;
- evaluarea riscurilor şi realizarea planului de audit;
- detalierea planului de audit;
- verificarea preliminară a ariei de audit;
- realizarea testelor de conformitate *(compliance test)* (adesea referite ca teste de control);
- realizarea testelor de fond *(substantive test)*;
- raportarea (comunicarea rezultatelor);
- urmărirea recomandărilor *(follow-up)*.

După prima etapă a procesului, cea de planificare, auditorul are o imagine mult mai clară asupra sistemului ce va fi auditat. Fondul de informaţii culese, analiza riscurilor şi evaluarea controalelor interne i-au permis identificarea zonelor critice ale sistemului auditat. Pe baza unui program de audit bine structurat, desfăşurarea misiunii se va axa pe desfăşurarea testelor de conformitate şi de fond care îi vor permite auditorului să obţină probe *suficiente* şi *relevante*, pentru fundamentarea concluziilor sale şi exprimarea unei opinii. În mod practic, acest proces de testare nu este exhaustiv, ci foloseşte tehnica de eşantionare.

Procesul de audit se finalizează prin elaborarea unui raport de audit, în cuprinsul căruia se vor regăsi opinia, concluziile şi recomandările auditorului SI.

1.4.1. Programul de audit

Programul de audit are la bază planul de audit, stabilit în etapa de planificare, şi el va servi, pe de o parte, ca un set de instrucţiuni adresat asistenţilor implicaţi în cadrul misiunii, iar pe de altă parte, ca un mijloc de control şi evidenţă a desfăşurării activităţii. Programul de audit, spre deosebire de planul de audit, stabileşte în detaliu lucrările necesare pentru implementarea strategiei, numărul de ore estimate pentru realizarea fiecărei lucrări şi persoanele responsabile de execuţia acestora.

Programul de audit identifică scopul, obiectivele şi procedurile de audit care se vor desfăşura pentru a se obţine probe suficiente şi relevante, necesare pentru a susţine concluziile şi opinia auditorului. Pentru fiecare procedură, programul prevede funcţiile şi aria pe care o vizează, prezentarea în detaliu a activităţilor care se vor desfăşura, tehnicile şi metodele pe care auditorul le va folosi, persoanele responsabile de execuţia lor şi fondul de timp asociat.

Tehnicile şi metodele folosite de auditorul SI în evaluarea şi testarea controalelor sistemului informaţional sunt:

- utilizarea software-ului generalizat de audit pentru analiza fişierelor de date (inclusiv fişierele de tip jurnal ale sistemului);
- utilizarea software-ului specializat pentru a determina modul de configurare a sistemului de operare (sau pentru a detecta deficienţe în stabilirea unor parametri);
- tehnica organigramelor pentru documentarea fluxului de activităţi din cadrul organizaţiei, cât şi a fluxurilor din cadrul aplicaţiilor informatice;
- utilizarea rapoartelor de audit din misiuni anterioare;
- verificarea documentaţiei sistemului;
- observarea.

Pe parcursul misiunii, în cadrul programului de audit pot apărea modificări în funcţie de rezultatele testelor şi analizelor sistemului auditat.

1.4.2. Eşantionarea

În general, din considerații de timp şi de cost, auditorul nu examinează totalitatea informaţiilor la care are acces pentru a-şi colecta elementele probante cu privire la sistemul de control intern, ci aplică o metodă tradiţională de selectare a datelor numită ***eşantionare***.

În audit, eşantionarea poate folosi atât o abordare *statistică*, cât şi una *nonstatistică*.

Eşantionarea statistică are în vedere, întotdeauna, întreaga populaţie şi este considerată o bază mai fundamentată pentru exercitarea raţionamentului profesional al auditorului, obiectivul metodei fiind determinarea mărimii eşantionului şi a criteriului de selectare.

Eşantionarea prin metode nestatistice implică o doză de subiectivism, bazându-se pe o selecţie făcută în funcţie de hazard – auditorul folosindu-şi raţionamentul profesional atât în determinarea mărimii eşantionului şi a criteriului de selecţie, cât şi în interpretarea rezultatelor.

Ambele metodele implică o serie de incertitudini concretizate într-un ***risc de eşantionare.*** Întotdeauna, auditorul este supus riscului de a ajunge la concluzii diferite de cele la care s-ar fi ajuns printr-un control exhaustiv.

În cadrul misiunii sale, auditorul poate aplica eşantionarea asupra:

- ***testelor de control***, pentru a se verifica rata de apariţie a întreruperii funcţionării unui control. Tehnica de eşantionare este cunoscută sub numele de ***eşantionarea atributelor*** (*attribute sampling*). Exemple de teste de control, unde eşantionarea este necesară, sunt: controlul drepturilor de acces ale utilizatorilor în sistem, verificarea existenţei aprobării/autorizării cererii de creare a unui cont de utilizator la nivelul unei aplicaţii/sistem de operare, controlul procedurilor de modificare a programelor, analiza fişierelor de tip jurnal;
- ***testelor de fond,*** când auditorul urmăreşte verificarea unei anumite valori din situaţiile financiare. Tehnica de eşantionare este cunoscută sub numele de ***eşantionarea variabilelor*** (*variable sampling*), iar un exemplu de test de fond este verificarea calculelor soldurilor finale pentru un eşantion de conturi.

Tehnica de eşantionare necesită un demers logic, implicând o succesiune de alegeri raţionale (precum mărimea eşantionului, gradul de precizie, nivelul de încredere) care, în final, pot aduce dovezi convingătoare în cazul unor arbitraje inerente. Utilizarea eşantioanelor în aplicarea testelor de audit implică, de regulă, următoarele etape:

1. determinarea obiectivelor testului ce va fi aplicat;
2. definirea populaţiei din care se va extrage eşantionul;
3. determinarea metodei de eşantionare;
4. calcularea mărimii eşantionului;
5. selectarea eşantionului;
6. evaluarea rezultatelor.

1. Determinarea obiectivului

Eficacitatea aplicării unei tehnici de eşantionare este determinată de definirea precisă a obiectivelor sale, auditorul subliniind ce urmăreşte să demonstreze, să probeze (spre exemplu, un astfel de obiectiv poate viza validitatea conturilor clienţilor organizaţiei auditate).

2. Determinarea populaţiei

Ansamblul datelor – în fapt, populaţia – asupra căruia auditorul doreşte să ajungă la o concluzie şi din care urmează să preleveze eşantionul corespunzător trebuie să fie în concordanţă cu obiectivul stabilit în etapa anterioară.

O analiză a populaţiei se impune a fi realizată şi ea vizează, pe de o parte, ***exhaustivitatea*** – completitudinea populaţiei considerate a fi supusă controlului şi, pe de altă parte, ***omogenitatea*** (natura şi structura) acesteia, pentru că o extrapolare a rezultatelor unui eşantion are valabilitate doar într-o populaţie rezonabil omogenă. În situaţia în care populaţia nu este omogenă, se impune ***stratificarea*** acesteia în vederea obţinerii unor rezultate pertinente, proces ce constă în divizarea unei populaţii în subpopulaţii, având caracteristici comune.

3. Calculul mărimii eşantionului

Literatura de specialitate, în speţă statistica, recunoaşte implicaţiile majore ale anumitor caracteristici în vederea determinării eşantionului:

- *coeficientul de încredere*, definit ca o expresie procentuală a probabilităţii că eşantionul ales este reprezentativ pentru populaţie. Un procent de 95%, spre exemplu, va avea implicaţii asupra mărimii eşantionului definindu-l ca un eşantion mare;
- *nivelul de risc* este complementul coeficientului de încredere, fiind exprimat ca:
- Nivelul de risc = 1- Coeficientul de încredere;
- Spre exemplu, dacă coeficientul de încredere este 95%, nivelul de risc este 5% (100%-95%);
- *precizia* este fixată de auditorul SI, ea reprezintă diferenţa acceptabilă de mărime dintre eşantion şi populaţia actuală. Pentru eşantionarea pe bază de atribute, această mărime este stabilită ca un procent. Pentru eşantionarea pe bază de variabile, această mărime este stabilită ca o valoare;
- *rata de eroare aşteptată* reprezintă o estimare în procente a erorilor care ar putea exista;
- *media eşantionului* este suma valorică a elementelor eşantionului împărţită la numărul de elemente ale acestuia;
- *deviaţia standard a eşantionului* calculează variaţia valorii eşantionului de la media eşantionului. Aceasta măsoară dispersia valorilor eşantionului;

- *eroarea tolerabilă* – este numărul maxim de erori dintr-o populaţie pe care auditorul SI este dispus să le accepte. În aplicarea testelor de control, acest parametru reprezintă rata maximă de deviaţie de la procedurile de control prescrise pe care auditorul SI o va accepta;
- *deviaţia standard a populaţiei* este un concept matematic care măsoară relaţia distribuţiei normale. Acest parametru este aplicat doar formulelor de eşantionare cu variabile (nu formulelor de eşantionare cu atribute).

O metodă de determinare a eşantionului[5], mult utilizată în practica cabinetelor de audit, este:

$$\textbf{\textit{Mărime eşantion}} = \frac{\text{Factor de încredere}}{\text{Eroarea tolerabilă}}$$

în care factorul de încredere este furnizat de tabelul 1.4.1 şi depinde de doi parametri: coeficientul de încredere şi numărul de erori aşteptate.

Tabelul 1.4.1. **Valorile asociate factorului de încredere**[6]

Numărul de erori	**Coeficientul de încredere asociat eşantionării**				
	70%	**80%**	**90%**	**95%**	**99%**
0	1.21	1.61	2.31	3.00	4.61
1	2.44	3.00	3.89	4.75	6.64
2	3.62	4.28	5.33	6.30	8.41
3	4.77	5.52	6.69	7.76	10.05

În acest context, un exemplu de determinare a mărimii unui eşantion, plecând de la premisele cunoscute:

Eroarea tolerabilă = 5%
Coeficientul de încredere = 95%
Nr. erori aşteptate = 0

} ⟶ Factor de încredere = 3,

conduc la următorul rezultat:

Mărimea eşantionului = 3 / 5% = 60 elemente

În termeni valorici, formula devine:

---

[5] ACCA, Study text – Accounting and Audit Practice, nr. 10, 2000.

[6] Prelucrare după I. Gray, S. Manson, *The audit process: principles, practice and cases*, ed. 2000.

$$\textit{Mărime eşantion} = \frac{\text{Valoarea populaţiei} \times \text{Factor de încredere}}{\text{Eroarea tolerabilă}}$$

În acest caz, considerându-se cunoscute datele de intrare:

Valoarea populaţiei = 5.000.000 u.m.

Eroarea tolerabilă = 200.000 u.m.
Coeficientul de încredere = 95%
Nr. erori aşteptate = 0

→ Factor de încredere = 3,

rezultatul final va fi:

Mărime eşantion = 3 × 5.000.000 / 200.000 = 75 elemente

4. Selectarea eşantionului

Principiul care guvernează procesul de selectare a elementelor dintr-o populaţie, în vederea formării unui eşantion, este acela că fiecare individ trebuie să aibă o şansă egală de a fi ales. Literatura de specialitate (statistica) recunoaşte diferite metode de selecţie:

- selecţie aleatorie;
- selecţie sistemică – ce urmăreşte tehnica: se stabileşte un punct de pornire, de la care, aplicând un pas fix se alege fiecare element;
- selecţie în bloc – alegerea spre exemplu dintr-un total de 100 de elemente pe cele corespunzătoare poziţiilor 55-70;
- selecţie pe bază de hazard „aşa-zisa alegere cu ochii închişi";

Odată stabilit eşantionul, auditorul va proceda la testarea rezultatelor acestuia, în conformitate cu obiectivele de audit stabilite.

5. Evaluarea rezultatelor

Erorile constatate asupra eşantionului se vor extrapola la populaţia din care a rezultat, metoda de extrapolare fiind întotdeauna compatibilă cu metoda de prelevare a eşantionului.

1.4.3. Probele de audit

Probele pentru audit reprezintă ansamblul documentelor, fişierelor şi observaţiilor obţinute în cursul misiunii de audit şi utilizate pentru elaborarea concluziilor şi formularea opiniei auditorului. Legislaţia în vigoare, inclusiv Standardele internaţionale de audit SI nu oferă un model standardizat al raportului de audit, al chestionarelor utilizate, al dosarului de audit, al foilor de lucru, ci pune un accent

deosebit pe raţionamentul profesional al auditorului. În acest sens, orice afirmaţie a acestuia trebuie să fie justificată şi documentată.

Standardul de audit ISACA „S14. Audit Evidence" recomandă auditorilor SI să obţină probe ***suficiente*** **şi** ***relevante***, pentru fundamentarea unor concluzii cât mai reale şi exprimarea unei opinii pertinente.

Principala condiţie a acestui volum semnificativ de documente este ***validitatea informaţiei*** pe care o conţine. Auditorul nu lucrează plecând de la ipoteze, ci se bazează pe certitudini astfel încât informaţiile culese să fie fiabile, relevante şi utile, iar constatările făcute să fie justificate şi, în consecinţă, incontestabile.

Caracterul just al elementelor probante se apreciază în funcţie de relevanţa şi fiabilitatea lor. În unele situaţii, auditorul se sprijină pe elemente probante care nu sunt concludente prin ele însele, dar care contribuie la definitivarea concluziilor. Certitudinea auditorului sporeşte în cazul în care elementele probante din surse diferite şi de naturi diferite sunt concordante între ele.

Fiabilitatea elementelor probante colectate este apreciată în funcţie de originea lor internă sau externă, de natura lor scrisă sau orală şi de circumstanţele în care s-au obţinut, astfel:

- probele de audit din surse externe (spre exemplu, confirmarea de la o terţă parte) sunt mai credibile decât cele obţinute din cadrul organizaţiei;
- probele de audit obţinute din cadrul organizaţiei sunt mai credibile atunci când controlul intern este de încredere;
- probele de audit obţinute direct de auditor sunt mai credibile decât cele obţinute din cadrul organizaţiei;
- probele de audit sub formă de documente scrise sunt mai credibile decât declaraţiile orale.

Determinante pentru evaluarea relevanţei probelor sunt şi:

- independenţa celui care furnizează probele – probele obţinute din exteriorul organizaţiei sunt mai credibile decât cele interne;
- calificarea indivizilor care furnizează probele/informaţiile;
- obiectivitatea probelor;
- „vârsta" probelor.

Probele pe care auditorul SI le culege într-o misiune sunt variate, iar tehnicile folosite în procesul de culegere a probelor sunt:

- verificarea structurilor organizatorice ale sistemului informatic. O structură organizatorică trebuie să asigure o separare a funcţiilor incompatibile;

- verificarea politicilor interne şi procedurilor de lucru;
- verificarea standardelor ce vizează domeniul IT;
- verificarea documentaţiei sistemului informatic. În mod practic, auditorii SI vor analiza:
  - documentaţia de dezvoltare a sistemului informatic (ex: studii de fezabilitate);
  - specificaţiile de proiectare şi cerinţele funcţionale;
  - documentele operaţionale;
  - fişierele de tip jurnal şi fişiere de tip istoric a modificării programelor sursă;
  - manualele utilizatorilor;
  - manualele de operare;
  - documentele relative la securitate (planuri de securitate, evaluarea riscurilor);
  - rapoartele de asigurare a calităţii;
- intervievarea personalului din departamentul IT;
- observarea performanţei sistemului şi a utilizatorilor săi.

1.4.4. Testele de audit

Pe parcursul desfăşurării misiunii de audit, pentru a culege probe cât mai relevante şi suficiente, auditorul SI desfăşoară două categorii de teste:

- ***teste de conformitate (teste de control),*** pentru a verifica conformitatea controlului intern cu politicile, normele interne stabilite de managementul organizaţiei;
- ***teste de fond*** pentru a verifica integritatea tranzacţiilor individuale, a datelor şi a altor informaţii din sistem.

Identificarea punctelor-cheie de control îi vor permite auditorului SI să extindă analiza lor preliminară, prin aplicarea testelor de conformitate, pentru a determina dacă ele lucrează aşa cum au fost planificate.

Având în vedere obiectivele controlului intern, care se pot rezuma în asigurarea validităţii, exhaustivităţii, acurateţei şi confidenţialităţii resurselor informaţionale dintr-o organizaţie, auditorul, prin intermediul testelor de conformitate, va verifica existenţa şi eficienţa controlului intern. Altfel spus, prin aceste teste, auditorul urmăreşte *conformitatea* controlului intern existent în cadrul organizaţiei cu politicile şi procedurile managementului, cât şi *consecvenţa* de aplicare a acestui control. Spre exemplu, atunci când auditorul SI va analiza separarea funcţiilor incompatibile din cadrul sistemului informatic, va selecta un eşantion de utilizatori pentru a le analiza drepturile de acces din cadrul sistemului cu drepturile înscrise în fişele lor de post.

Evaluarea controlului intern, prin analiza rezultatelor testelor de conformitate desfăşurate, va influenţa proiectarea şi desfăşurarea testelor de fond. În mod practic, există o relaţie direct proporţională între nivelul controlului intern şi volumul testelor de fond ce sunt necesare a fi desfăşurate. Dacă rezultatele testelor de conformitate conferă prezenţa unui control intern eficient, atunci auditorul SI va aplica un număr minim de teste de fond. În caz contrar, dacă testarea controlului intern relevă slăbiciuni ale acestuia, atunci, pentru verificarea completitudinii, acurateţei şi validităţii informaţiilor generate de sistemul informatic, testele de fond sunt o necesitate.

Testele de fond dovedesc integritatea procesării curente. În mod practic, un astfel de test va oferi probe asupra validităţii şi integrităţii situaţiilor financiare, cât şi a tranzacţiilor incluse în aceste situaţii. În general, auditorul SI utilizează testele de fond pentru a identifica erorile valorice care afectează situaţiile financiare. Spre exemplu, auditorul SI poate aplica un test de fond pentru a determina dacă înregistrările de la inventar sunt stabilite în mod corect. Rezultatele acestui test vor oferi probe ce-l pot determina pe auditor să se exprime asupra acurateţei inventarului realizat.

Testele de conformitate nu se substituie testelor de fond, iar figura 1.4.1 relevă legătura ce se stabileşte între cele două categorii de teste.

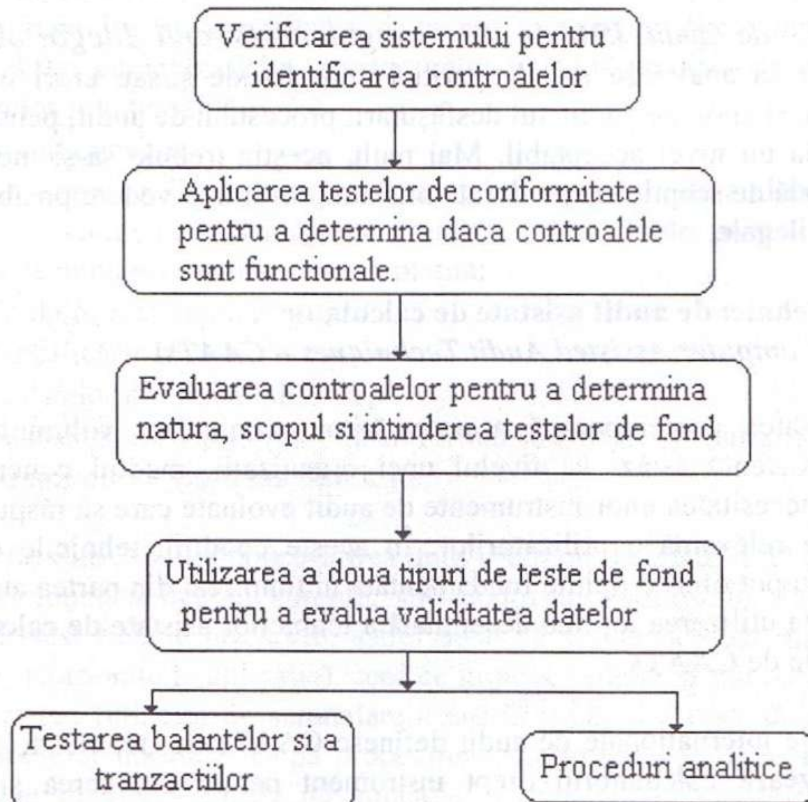


Figura 1.4.1. **Relaţia dintre testele de conformitate şi testele de fond**

1.4.5. Detectarea fraudei

Într-un cadru general, frauda poate fi definită ca un act de rea-credinţă săvârşit de o persoană, de obicei pentru a realiza un profit material de pe urma afectării drepturilor altuia, adică o acţiune comisă cu intenţia de a înşela. Normele internaţionale de audit menţionează că termenul de „fraudă se referă la o acţiune cu caracter intenţionat întreprinsă de una sau mai multe persoane din rândul conducerii, al salariaţilor sau terţilor, acţiune ce are ca efect o interpretare eronată a situaţiilor financiare".

Încă din etapa de planificare, auditorul trebuie să evalueze riscul apariţiei unor fraude şi erori, pentru că, în general, frauda implică acţiuni mascate, ceea ce determină ca unele erori semnificative să nu fie descoperite, iar auditorul să formuleze o opinie eronată. Ceea ce sporeşte riscul de fraudă sunt carenţele funcţionale ale sistemului de control intern. Noel Pons[7] enunţa un principiu esenţial pe care auditorii, în special auditorii interni, nu trebuie să-l uite: „frauda creşte din lipsă de transparenţă" şi, tocmai de aceea, cea mai bună prevenire a fraudei este controlul intern.

Responsabilitatea pentru prevenirea şi detectarea fraudelor aparţine conducerii, auditorul SI putând juca un rol pozitiv în prevenirea acestora, dar nu el are responsabilitatea de a detecta şi demonstra frauda.

Standardul de audit ISACA „S9. Irregularities and Illegal Acts" recomandă auditorilor să analizeze riscul apariţiei unor fraude şi/sau erori încă din etapa de planificare şi apoi, pe parcursul desfăşurării procesului de audit, pentru a reduce riscul de audit la un nivel acceptabil. Mai mult, aceştia trebuie să-şi menţină o atitudine profesională de scepticism pe durata misiunii, având în vedere posibilitatea existenţei unor acte ilegale.

1.4.6. Tehnici de audit asistate de calculator *(Computer Assisted Audit Techniques – CAATs)*

Complexitatea contemporană a activităţilor economice, volumul considerabil al datelor existente astăzi la nivelul unei organizaţii, mediul concurenţial activ au subliniat necesitatea unor instrumente de audit evoluate care să răspundă „foamei" de informaţie relevantă a utilizatorilor. În aceste condiţii, tehnicile clasice de audit, singure, nu pot oferi o opinie fundamentată în timp real din partea auditorului, fapt ce a condus la utilizarea tot mai accentuată a tehnicilor asistate de calculator, cunoscute sub numele de **CAATs**.

Standardele internaţionale de audit definesc CAATs ca „tehnici folosite de auditorii care utilizează calculatorul drept instrument pentru culegerea şi analiza datelor

[7] Citat în Renaerd J., *Teoria şi practica auditului intern*, Edition d 'Organisation, Paris, 2002.

necesare auditului". Astăzi, când sistemele informatice au diferite platforme hardware şi software, diferite structuri de date, funcţii de procesare, formate de înregistrare a tranzacţiilor etc., este aproape imposibil ca auditorii să colecteze probe fără un instrument software de analiză a datelor.

Aceste instrumente şi tehnici moderne pot asista auditorul în orice etapă a misiunii sale, fiind utilizate pentru:

- testarea măsurilor de securitate dintr-un sistem;
- analiza şi controlul aplicaţiilor informatice existente în sistem;
- identificarea riscurilor unei organizaţii şi evaluarea acestora;
- evaluarea controlului intern;
- verificarea integrităţii fişierelor;
- analiza informaţiilor clientului auditat prin interogări complexe ale bazelor de date, extrageri, stratificări, totalizări.

CAATs includ multe tipuri de instrumente şi tehnici, cum ar fi software generalizat de audit, testul de date, testul integrat, aplicaţii software de urmărire şi mapare şi sisteme expert.

Software generalizat de audit (*Generalized Audit Software: GAS*) este reprezentat de pachete de programe ce au capacitatea de a citi şi extrage direct datele din platforme diferite. Deşi caracteristicile acestor aplicaţii sunt nuanţate, ele permit realizarea următoarelor funcţionalităţi:

- selectarea eşantioanelor;
- manipularea, sortarea datelor conform cerinţelor exprimate de auditor; astfel de operaţii pot scoate în evidenţă, spre exemplu, plăţile duble, printr-o sortare a datelor după numărul facturii şi suma plătită;
- testarea calculelor matematice;
- totalizări, stratificări;
- compararea datelor din fişiere diferite;
- listarea rapoartelor sau scrisorilor într-un format specificat de auditor;
- detectarea tranzacţiilor lipsă sau duplicate.

Tehnica „testului de date" necesită pregătirea unui eşantion de „date-test" pentru a fi procesate de versiunea aplicaţiei curente, sub controlul auditorului. Datele şi, implicit, tranzacţiile-test trebuie proiectate astfel încât să se verifice cât mai multe controale posibile (încorporate în aplicaţie), ceea ce impune utilizarea atât a unor ***date invalide***, pentru testarea rutinelor de semnalare a erorilor, cât şi a unor ***date valide*** pentru testarea proceselor normale. După procesarea eşantionului de date, auditorul va urmări şi aprecia mesajele afişate de aplicaţie, va analiza controalele interne

încorporate în sistem, va compara rezultatele procesării cu cele calculate manual. Proiectarea unui bun test de date este obiectivul major al acestei tehnici.
Auditorii pot utiliza astfel de teste pentru verificarea aplicaţiilor contabile şi evaluarea controalelor aferente sistemelor precum:

- controlul accesului la date şi alte controale specifice (exemplu: parole on-line);
- controlul validării datelor de intrare, controlul totalurilor (restricţii de integritate încorporate);
- erori logice în procesarea tranzacţiilor;
- acurateţea calculelor matematice.

Testul integrat (*Integrated Test Facility: ITF*)
Utilizarea unui ITF permite auditorului să introducă date fictive, fără ştiinţa utilizatorilor, pentru a verifica eficienţa sistemului. Facilitatea pe care o oferă testul presupune crearea unor fişiere principale-fictive în cadrul sistemului informatic; la intervale aleatorii de timp, auditorul introduce „datele de testat" care vor fi procesate de aplicaţie, dar care vor actualiza fişierele fictive, astfel încât procesarea datelor curente ale firmei nu va fi afectată (spre exemplu, introduce un angajat fictiv, iar toate operaţiile din aplicaţie se execută asupra acestuia, evaluându-se acurateţea şi integritatea prelucrărilor din aplicaţie).

Principalul avantaj al acestui test constă în posibilitatea auditorului de a procesa tranzacţii fictive, în acelaşi timp cu tranzacţiile reale ale organizaţiei. Spre deosebire de tehnica datelor de test, în acest caz auditorul este sigur că versiunea programului testat este aceeaşi cu cea folosită la procesarea datelor firmei. Adesea, utilizarea unui astfel de test presupune o modificare a aplicaţiei de bază pentru identificarea tranzacţiilor fictive. Astfel, auditorul trebuie să se asigure că programatorul care se ocupă de această activitate nu va modifica aplicaţia, astfel încât controalele să se efectueze asupra tranzacţiilor fictive, şi nu asupra celor reale.

Tehnici pentru analiza fluxurilor de date din cadrul unui sistem sau al unei aplicaţii informatice.
Instantaneu (Snapshot) reprezintă o facilitate ce permite auditorului să „îngheţe" programul într-un anumit punct, pentru a verifica valorile unei tranzacţii şi prelucrările efectuate în timpul funcţionării programului. Tehnica propriu-zisă este rapidă şi uşor de utilizat, deşi are o funcţie limitată şi specifică, ea oferind auditorului un nivel de reasigurare asupra controalelor interne din cadrul sistemului. Un exemplu de „vedere punctuală" ar fi o linie de cod dintr-un program ce produce un blocaj, acest blocaj conducând la obţinerea unei valori eronate.

Urmărirea (Tracing) presupune generarea unui traseu de audit complet pentru urmărirea tranzacţiilor în timpul prelucrărilor. Prin executarea unei „urmăriri" este

posibil să se sesizeze ce efect are fiecare linie de cod asupra fiecărei date prelucrate. Dacă programul nu prelucrează toate tranzacţiile în mod corect, în momentul în care intervine eroarea, aceasta va fi evidenţiată în mod distinct. Principalul avantaj al tehnicii este acela că auditorul poate vedea anumite etape ale programului care în mod obişnuit se derulează foarte rapid. Dezavantajele „urmăririi" rezidă din faptul că auditorul are nevoie de cunoştinţe de programare şi că funcţiile de „urmărire" pot varia de la produs la produs.

Maparea (Mapping) presupune monitorizarea execuţiei unui program în scopul stabilirii unor informaţii statistice, cum ar fi spre exemplu: cod de program neexecutat, de câte ori au fost executate anumite linii din program. Auditorul poate utiliza „maparea" pentru a evidenţia codul redundant sau codul utilizat în scopuri frauduloase.

Inteligenţa artificială şi sistemele expert

CAATs prezentate mai sus pot juca un rol important în cadrul unei misiuni de audit, şi totuşi capacitatea lor de a asista auditorul în domeniul „judecăţilor" este extrem de limitată. Cea mai mare provocare o constituie pentru activitatea de audit – ca şi pentru orice domeniu managerial – luarea deciziilor de către expertul uman. Judecata auditorului include raţionamente, referiri la cazuri trecute sau la cazuri ipotetice, creativitate şi, nu în ultimul rând, intuiţie.

Sistemele expert, definite ca „produse program, care emulează comportamentul experţilor umani, în rezolvarea unor probleme din lumea reală asociate unui domeniu particular al cunoaşterii"[8], se remarcă astfel ca fiind instrumente extrem de utile auditorului în cadrul misiunii sale: planificarea auditului, evaluarea controlului intern (în scopul de a estima gradul de siguranţă pe care îl poate acorda controlului intern efectuat de organizaţia respectivă), analiza riscurilor. Un sistem expert, prin intermediul motorului de inferenţă, va oferi sugestii cu privire la procedurile specifice care pot fi întreprinse.

Avantajele generale oferite de aceste instrumente sunt:

- productivitate crescută prin reducerea ciclului de audit; concentrarea timpului pe funcţii critice; operaţii simplificate datorită automatizării;
- îmbunătăţirea calităţii auditului, datorită auditării 100% a datelor şi standardizării metodelor de audit;
- creşterea valorii clientului prin recuperarea veniturilor pierdute. Analiza în detaliu a tuturor datelor poate descoperi multe pierderi, anomalii;

---

[8] Pigford, D.V., Baur, G., *Expert Systems for Business. Concepts & Applications,* 2nd edition Boyd and Fraser Publishing, 1995.

- reducerea timpului de realizare a misiunii de audit, deoarece se accelerează identificarea excepţiilor, se simplifică pregătirea foilor de lucru, rapoartele se generează automat;
- asigură avantaje imediate clientului auditat prin reducerea riscului de zi cu zi; detectarea iregularităţilor şi fraudelor; analiza datelor ce pot constitui prognoze;
- asigurarea unei independenţe mai mari faţă de mediul auditat;
- reducerea cheltuielilor în timp.

Alături de avantajele subliniate, este necesar să menţionăm că instrumentele de tip CAAT au şi limite, cum ar fi:

- cerinţele de specializare sunt costisitoare;
- anumite CAAT sunt foarte generale astfel încât adaptarea lor poate fi un proces dificil;
- incompatibilitatea anumitor CAAT cu sistemul informatic al clientului (situaţii în care este esenţială alegerea pe care o face auditorul).

1.4.7. Raportul de audit

Raportul de audit reprezintă instrumentul prin care se comunică obiectivele auditării, normele/standardele aplicate, constatările şi concluziile misiunii. Această ultimă etapă de raportare are ca scop punerea în evidenţă a slăbiciunilor controalelor analizate de auditorul SI şi aducerea lor la cunoştinţă, prin intermediul raportului de audit, care va conţine sinteza principalelor constatări şi recomandări.

Standardele ISACA de audit SI, S7 „Reporting" şi S8 „Follow-up Activities" oferă elemente de bază pentru realizarea acestui document. Aceste standarde recomandă ca, la sfârşitul misiunii de audit, auditorul SI să furnizeze un raport care va identifica organizaţia auditată, destinatarii raportului şi orice restricţie de circulaţie a acestuia.

Chiar dacă normele legale nu impun utilizarea unui raport standardizat, în practică, se regăseşte o tendinţă spre a formaliza conţinutul acestui raport tocmai pentru a asigura o bună înţelegere şi o identificare uşoară a elementelor semnificative din partea utilizatorului final. În acest sens, raportul de audit trebuie să aibă o anumită structură şi un conţinut ce vor include elementele de bază:

- partea introductivă a raportului, va include scopul auditării, obiectivele urmărite, perioada acoperită, natura şi întinderea procedurilor de audit;
- în cuprinsul său, se regăsesc:
  - opinia şi concluziile misiunii;
  - orice rezervă pe care auditorul o are asupra sistemului auditat;
  - detalii asupra unor constatări semnificative şi recomandările necesare, limitările auditului:

- un paragraf prin care se precizează că din cauza limitelor inerente ale controalelor interne, frauda sau erorile pot să apară sau să rămână nedectate;
- un paragraf prin care se precizează că auditul nu poate detecta toate punctele slabe din cadrul procedurilor de control atât timp cât nu este o activitate continuă, iar testarea procedurilor de control de către auditor se realizează prin sondaj;

▪ standardele, ghidurile şi normele asociate domeniului auditat ce au constituit referenţialul de raportare pentru auditor;

♦ în partea finală a raportului, se înscriu data raportului, adresa şi semnătura auditorului.

Între recomandările standardelor internaţionale de audit SI, menţionăm de asemenea că raportul de audit trebuie semnat şi realizat în termenul stabilit prin contractul de audit sau scrisoarea de angajament.

1.5. Perspective privind auditul sistemelor informaţionale

Astăzi, într-o eră informatizată, apare necesitatea exprimării, de către auditor, a unei opinii fundamentate în timp real, în defavoarea abordării clasice, cu caracter istoric. Dezvoltarea şi integrarea tot mai accelerată a tehnologiei informaţiei la nivelul oricărei organizaţii a avut implicaţii majore şi în domeniul auditului, prin dezvoltarea unor noi abordări, tehnici şi metode precum: autoevaluarea controlului intern (*control self assessment*), abordarea integrată şi auditul continuu.

Auditorul trebuie să aprecieze calitativ informaţia produsă de sistemele informaţionale, solicitarea venind, în acest sens, atât din partea managementului intern, cât şi din partea acţionarilor externi care simt nevoia să fie informaţi pentru a rezista mediului concurenţial.

1.5.1. Autoevaluarea controlului (*Control Self Assesment*)

Autoevaluarea controlului reprezintă o tehnică de management care asigură acţionarii, clienţii şi alţi parteneri că sistemul de control al unei organizaţii este de încredere. Mai mult, utilizarea acestei tehnici îi va determina pe angajaţii organizaţiei să se implice mai mult în procesul de evaluare a riscurilor organizaţiei şi verificare proactivă a controalelor. În mod practic, controlul de autoevaluare este o metodologie utilizată pentru a se verifica obiectivele-cheie ale organizaţiei, riscurile implicate în realizarea acestora şi controalele interne proiectate să reducă aceste riscuri la un nivel acceptabil. Implementarea acestei tehnici se poate realiza cu o serie de instrumente, plecând de la simple chestionare la workshop-uri interactive, proiectate pentru a culege informaţii despre organizaţie.

În literatura de specialitate, autoevaluarea controlului este considerată un instrument proiectat să asiste funcţia de audit intern şi să testeze eficienţa controlului intern. O definiţie clară, coerentă asupra conceptului de CSA nu există, însă mulţi autori l-au descris astfel:

- CSA este un program de management al riscurilor în care riscurile şi controalele sunt examinate şi evaluate pentru a oferi managementului o asigurare rezonabilă ca obiectivele organizaţiei vor fi realizate. Responsabilitatea programului CSA este împărţită între toţi angajaţii;[9]
- CSA este o autoevaluare întreprinsă asupra unui sistem (aplicaţie majoră sau sistem de utilizare generală), sau un set de autoevaluări întreprinse pentru un grup de sisteme interconectate (interne sau externe fata de organizaţie). Este o metodă folosită pentru a măsura asigurarea securităţii IT, gradul de încredere asupra măsurilor de securitate, tehnice şi operaţionale luate pentru a proteja sistemul şi informaţiile pe care acesta le procesează;[10]
- CSA impune angajaţilor şi managerilor implicaţi direct în activitatea afacerii să determine dacă procesele în curs sunt efective şi dacă obiectivele sunt realizate;
- din punctul de vedere al managementului superior, CSA sprijină demersul de estimare a măsurii în care organizaţia este pe cale să-şi îndeplinească obiectivele. Avantajele majore ale implementării CSA sunt detectarea timpurie a riscurilor şi dezvoltarea de planuri concrete de acţiune care protejează programele organizaţiei împotriva riscului semnificativ al afacerii. Scopurile CSA sunt:
  - reducerea sau eliminarea controalelor costisitoare şi ineficiente în timp;
  - localizarea precisă a zonelor de risc odată cu dezvoltarea evaluărilor adecvate ale controalelor;
  - evaluarea standardelor de control existente;
  - sublinierea responsabilităţii managementului pentru dezvoltarea şi monitorizarea sistemelor interne de control;
  - comunicarea rezultatelor.[11]

Un program CSA poate fi implementat prin diferite metode. În mod practic, nu este recunoscut un model clasic de dezvoltare şi implementare, fiecare organizaţie realizându-l în funcţie de particularităţile controlului intern. Fiecare program CSA are un ciclu de viaţă (prezentat în figura 1.5.1), în cadrul căruia, pe baza analizelor şi evaluărilor dezvoltate, chestionarele se pot reajusta în funcţie de necesităţi.

---

[9] Doughty, Ken, *Control self assessment*, 2001.
[10] Security Self Assessment Guide for Information Technology Systems (NIST – www.nist.gov)
[11] www.internalcontrols.uci.edu

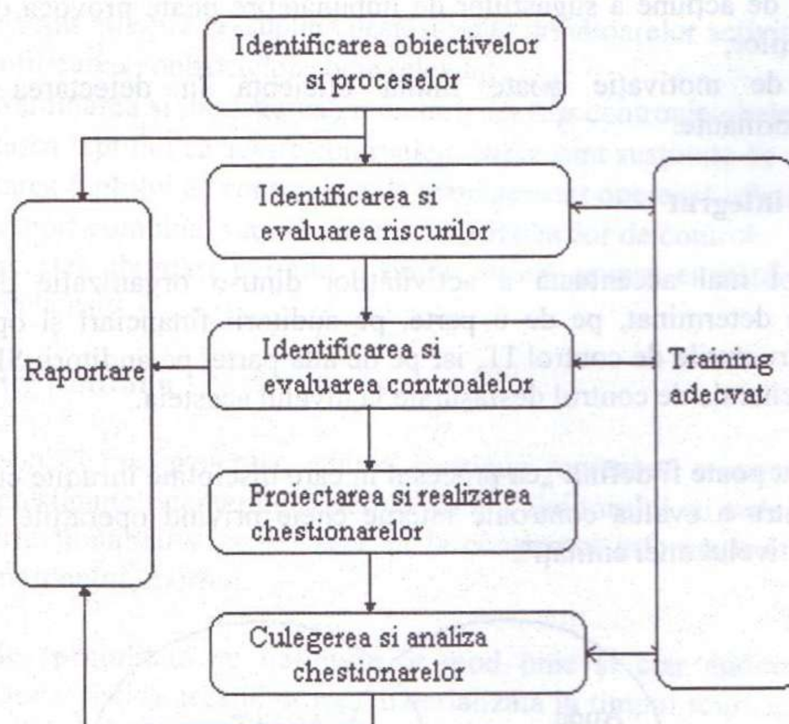


Figura 1.5.1. **Ciclul de viaţă al unui CSA**

Avantajele acestei tehnici, de autoevaluare a controlului intern sunt:

- detectarea timpurie a riscurilor;
- desfăşurarea unor controale interne mai eficiente şi mult îmbunătăţite;
- constituirea unor echipe de lucru bine închegate, eficiente;
- creşterea interesului angajaţilor în obiectivele organizaţionale şi a cunoştinţelor despre riscuri şi controale interne;
- îmbunătăţirea comunicaţiei dintre nivelul operaţional şi top-managementul organizaţiei;
- îmbunătăţirea evaluării procesului de audit;
- reducerea costurilor asociate controalelor;
- siguranţa oferită acţionarilor şi clienţilor;
- siguranţa necesară oferită de top management cu privire la suficienţa controalelor interne, în conformitate cu Sarbanes-Oxley Act.

Alături de avantajele prezentate, este necesar să subliniem şi dezavantajele CSA:

- poate fi greşit înţeleasă ca un înlocuitor pentru funcţia de audit;
- este privită ca o muncă adiţională – un raport în plus trimis către management;

- eşecul de acţiune a sugestiilor de îmbunătăţire poate provoca demoralizarea angajaţilor;
- lipsa de motivaţie poate limita eficienţa în detectarea controalelor neperformante.

1.5.2. Auditul integrat

Dependenţa tot mai accentuată a activităţilor dintr-o organizaţie de tehnologia informaţiei i-a determinat, pe de o parte, pe auditorii financiari şi operaţionali să aprofundeze structurile de control IT, iar pe de altă parte, pe auditorii SI să analizeze şi structurile generale de control desfăşurate la nivelul acesteia.

Auditul integrat poate fi definit „ca procesul în care discipline înrudite cu auditul sunt combinate pentru a evalua controale interne cheie privind operaţiile şi procesele desfăşurate la nivelul unei entităţi".

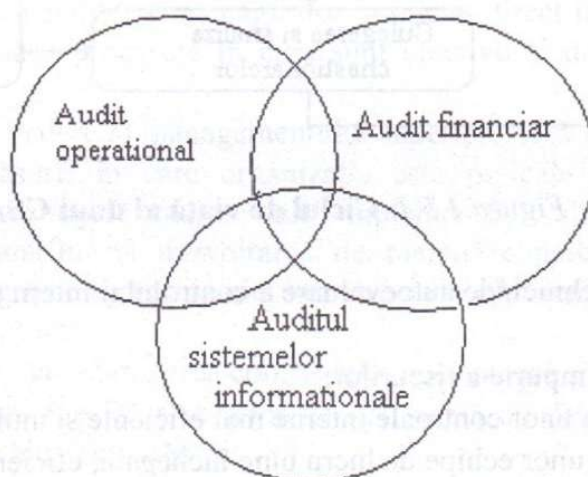


Figura 1.5.2. **Auditul integrat**

Abordarea auditului integrat este o abordare bazată pe risc. Un element-cheie al abordării integrate este discutarea tuturor riscurilor apărute în sistem, fie ele financiare, operaţionale sau informatice, cu toţi membrii echipei de audit, proces care va analiza impactul şi probabilitatea de realizarea a fiecărui risc semnificativ.

În acest context, auditorului SI va desfăşura o înţelegere şi o identificare a riscurilor din arii precum managementul informatic, infrastructura IT, guvernanţa IT. Sistemele IT implică, în general, implementarea unui prim nivel de controale detective şi preventive, iar abordarea integrată va realiza o evaluare corectă a eficienţei şi eficacităţii lor.

Procesul de audit integrat presupune desfăşurarea următoarelor activităţi:

- identificarea controalelor-cheie relevante;
- reexaminarea şi înţelegerea proiectării acestor controale-cheie;
- testarea faptului că aceste controalele-cheie sunt susţinute de sistemul IT;
- testarea faptului că controalele de management operează eficient;
- un raport combinat sau o opinie asupra riscurilor de control.

Utilizarea acestei abordări permite o opinie unică asupra entităţii auditate, cu un raport comprehensiv.

1.5.3. Auditul continuu

Într-o perspectivă mai generală, auditul continuu reprezintă o metodă modernă de audit, care presupune interacţiunea permanentă a auditorului cu sistemul organizaţiei auditate, perfecţionându-se astfel accesul la conţinutul informaţional şi prezentarea acestuia la momentul oportun.

Literatura de specialitate nu defineşte în mod unic şi clar auditul continuu, dar subliniază caracteristica acestui proces materializată în timpul scurt scurs între faptele de auditat, colectarea probelor şi raportul de audit.

Dezvoltarea acestui concept a apărut şi din nevoia unei monitorizări în timp real a tuturor tranzacţiilor ce au loc la nivelul unei organizaţii, tocmai pentru a se înlătura dezastre financiare şi scandaluri, cum au fost Enron şi WorldCom. În mod practic, un audit continuu implică o muncă mai amplă de analiză şi evaluare deoarece el nu oferă doar un raport la sfârşitul unui trimestru, ci va oferi rapoarte mult mai frecvente.

În cadrul acestui proces, instrumentele şi tehnicile de audit trebuie să opereze în paralel cu procesarea tranzacţiilor, culegând datele în timp real, şi permit detectarea trendurilor şi a excepţiilor (spre exemplu, tranzacţii cu valori mult mai mari sau mult mai mici decât cele obişnuite), eventualele erori sau fraude. Acest proces de analiză complexă, implică utilizarea unor tehnici informatice avansate, cum ar fi tehnicile OLAP, Data Mining, reţele neuronale şi inteligenţa artificială.

Complexitatea instrumentelor software utilizate în cadrul unui audit continuu este recunoscută şi, în mod practic, ea include:

- instrumente de interogare;
- statistica şi analiza datelor (CAAT);
- sisteme de gestionare a bazelor de date (DBMS);
- depozite de date, data mining;
- inteligenţa artificială (AI);
- module de audit împachetate (EAM);
- tehnologii de tip reţele neuronale;
- standarde precum XBRL.

Pentru a înţelege implicaţiile şi necesităţile unui audit continuu, este necesar să se analizeze caracterul distinct dintre ***auditul continuu şi monitorizarea continuă***.

Monitorizarea continuă oferă managerilor IT o gamă de instrumente software specializate, care le va permite o supraveghere continuă a resurselor sistemului. Spre exemplu, un program antivirus în timp real sau un sistem de detectare a intruziunilor (IDS) sunt instrumente ce asigură o monitorizare continuă a unui sistem.

Auditul continuu – „o metodologie în care auditori independenţi oferă o asigurare scrisă asupra unui subiect utilizând o serie de rapoarte generate instantaneu, sau la o scurtă perioadă de timp, faţă de momentul producerii evenimentului respectiv". Realizarea unui audit continuu se bazează în mod clar pe proceduri automate de audit realizate prin tehnici şi instrumente software specializate.

În acest sens, auditul continuu trebuie sa fie independent de un control continuu sau o monitorizare continuă a activităţilor.

În general, se impune un set de *precondiţii* pentru desfăşurarea unui audit continuu:
- grad înalt de automatizare;
- un proces de producere a informaţiilor automatizat şi de încredere despre subiectul respectiv, la scurt timp după petrecerea evenimentului;
- alarme pentru a raporta în scurt timp eşecuri ale controlului;
- informarea rapidă a auditorilor asupra rezultatelor procedurilor automate, în mod particular când procesul identifică anomalii sau erori;
- disponibilitatea probelor de încredere;
- evaluarea factorilor de cost;
- auditori SI de formaţie tehnică;
- generarea rapidă a rapoartelor de audit automate;
- implementarea de instrumente de audit automatizate de nivel înalt care necesită ca auditorul sa fie implicat în setarea variabilelor/parametrilor.

Astăzi, instrumentele de monitorizare şi audit continuu sunt deja încorporate în aplicaţii de tip ERP, sistemele de operare şi pachetele de securitate de reţea. Configurarea adecvată a acestor sisteme va permite semnalarea situaţiilor critice, excepţiilor, în timp ce se operează cu datele din sistem. Prin urmare, ele reprezintă o instanţă a auditului continuu.

Mediul informatizat este un mediu natural pentru dezvoltarea şi realizarea unui audit continuu, datorită naturii intrinseci automate a proceselor.

1.6. Test de evaluare a cunoştinţelor

1. Un auditor SI evaluează accesul la o aplicaţie pentru a determina dacă ultimii zece utilizatori nou-creaţi au fost corect autorizaţi. Acesta este un exemplu pentru:
   a. eşantionare variabilă;
   b. testare de fond;
   c. testare de conformitate;
   d. eşantionare oprit/pornit (*stop-or-go sampling*).

2. Utilizarea procedurilor de eşantionare statistică duce la minimizarea:
   a. riscului de eşantionare;
   b. riscului de detecţie;
   c. riscului inerent;
   d. riscului de control.

3. Un element-cheie în analiza riscului este:
   a. planificarea auditului;
   b. controalele;
   c. vulnerabilităţile;
   d. responsabilităţi.

4. Care dintre următoarele teste sunt efectuate de auditorul SI atunci când un eşantion de programe este selectat pentru a determina dacă versiunile-sursă şi obiect sunt aceleaşi?
   a. un test de fond al controalelor bibliotecilor de programe;
   b. un test de conformitate al controalelor bibliotecilor de programe;
   c. un test de conformitate al controalelor compilatorului de program;
   d. un test de fond al controalelor compilatorului de program.

5. În conceptul de audit bazat pe risc, un auditor SI ar trebui în primul rând să efectueze:
   a. evaluarea riscului inerent;
   b. evaluarea riscului de control;
   c. test de evaluare a controlului;
   d. evaluarea testului de fond.

6. În planificarea auditului, pasul cel mai critic este identificarea:
   a. ariilor de riscuri majore;
   b. abilităţilor personalului auditor;
   c. paşilor testului în audit;
   d. timpului alocat auditului.

7. Când se implementează sisteme de monitorizare continuă, primul pas pe care îl face auditorul SI este să identifice:
   a. pragurile-ţintă rezonabile;
   b. ariile de risc majore din organizaţie;
   c. locaţia şi formatul fişierelor de ieşire;
   d. aplicaţiile care furnizează cel mai înalt potenţial de rambursare (*payback*).

8. Vicepreşedintele Departamentului resurselor umane a cerut un audit pentru anul trecut, pentru a identifica dacă au fost achitate salarii necuvenite. Care este cea mai bună tehnică de audit ce trebuie folosită în această situaţie?
   a. testarea datelor;
   b. software generalizat de audit (GAS);
   c. facilitate de test integrat (ITF);
   d. module de audit încorporate.

9. În cursul analizei riscurilor, un auditor a identificat ameninţări şi impacturi potenţiale. Următorul pas pe care îl realizează un auditor ar trebui să fie:
   a. identificarea şi evaluarea procesului de evaluare a riscului folosit de conducere;
   b. identificarea activelor informaţionale şi a sistemelor aferente;
   c. descoperirea ameninţărilor şi impacturile asupra conducerii;
   d. identificarea şi evaluarea controalelor existente.

10. Care dintre următoarele dovezi este cea mai concludentă pentru un auditor SI:
   a. o scrisoare de confirmare primită de la o terţă persoană pentru verificarea unui cont în balanţă;
   b. asigurarea din partea conducerii că aplicaţia lucrează aşa cum a fost proiectată;
   c. date de actualitate, obţinute din surse de pe internet;
   d. raportul de analiză al unui auditor SI, furnizat de conducere.

Capitolul 2

Guvernanță corporativă

Capitolul 2

Guvernanță corporativă

2.1. Guvernanță corporativă și guvernanță IT

Guvernanța corporativă, văzută ca setul de responsabilități și practici de conducere a unei entități în vederea realizării obiectivelor strategice ale acesteia, prin gestionarea corespunzătoare a riscurilor și a resurselor materiale și umane ale societății, constituie conceptul de bază al managementului tuturor activităților sociale.

În contextul în care guvernanța corporativă presupune conducerea activităților societății în condiții de transparență totală asupra riscurilor asociate activității acesteia, în condițiile protecției totale a tuturor drepturilor asociaților (partenerilor sociali), auditul, sub toate formele de manifestare ale acestuia, reprezintă garanția realizării acestor obiective.

Principiile guvernanței corporative se referă în principal la:

- crearea condițiilor de bază pentru o guvernanță corporativă funcțională;
- drepturile acționarilor și funcțiile-cheie ale dreptului de proprietate;
- tratamentul echitabil al acționarilor;
- rolul acționarilor în guvernanța corporativă;
- raportare și transparență;
- responsabilitățile consiliului de administrație.

CISA definește guvernanța corporativă drept „comportamentul etic al organizației asigurat de directori sau alte persoane cu responsabilități pe linia conducerii în crearea și prezentarea bogăției/averii organizației pentru toate persoanele deținătoare de interese legate de organizație".

OECD definește guvernanța corporativă ca fiind „distribuția drepturilor și responsabilităților între diferiții participanți în cadrul organizației, cum ar fi consiliul de administrație, managerii, acționarii, deținătorii de interese, care stabilesc reguli și proceduri în vederea luării deciziilor privind activitatea organizației". Prin aceasta se

realizează și stabilirea structurii prin care obiectivele organizației sunt stabilite și mijloacele pentru realizarea obiectivelor și monitorizarea performanțelor. Pentru realizarea tuturor acestor cerințe este necesară stabilirea de reguli privind administrarea și raportarea riscurilor, ceea ce impune în egală măsură un sistem de control intern eficient în vederea monitorizării riscurilor și îmbunătățirea activității.

În multe organizații, tehnologia informațională este considerată o parte integrantă a afacerii și este privită ca un factor de susținere și dezvoltare a acesteia. Consiliile de administrație și managerii executivi trebuie să extindă guvernanța și asupra IT și să asigure conducerea, structurile organizatorice și procesele care să permită organizației ca, prin componenta IT, să susțină și să extindă strategiile și obiectivele organizației. Expectația conducerii organizațiilor este ca tehnologia informațională să crească valoarea afacerii, să genereze mutații în direcția creșterii valorii, eficienței și productivității.

În contextul de mai sus, guvernanța IT acceptată ca „activitatea de conducere și coordonare a activității IT dintr-o organizație” devine o parte componentă a guvernanței corporative. Dacă inițial guvernanța corporativă era orientată spre transparență privind riscurile și protecția investiției acționarilor, prin folosirea extinsă a tehnologiei informaționale s-a creat o dependență de componenta IT, fapt ce impune concentrarea atenției asupra guvernanței IT.

Guvernanța IT este un concept care include sisteme informaționale, tehnologie și comunicații, probleme vizând businessul, aspecte legale, toate acestea privind deținătorii de interese, directorii, managementul superior, proprietarii proceselor, furnizorii IT, utilizatorii finali și auditorii. Guvernanța IT asigură alinierea funcției IT la obiectivele organizației. Funcția IT trebuie guvernată în baza cerințelor de bună practică pentru a se asigura faptul că informațiile și tehnologia implicată de acestea reprezintă un suport pentru activitatea organizației, resursele ei sunt folosite eficient și riscurile specifice sunt administrate corespunzător.

Tehnologia informației a fost considerată mult timp doar o componentă-suport pentru strategia organizației. Acum însă, este înțeleasă ca fiind o parte integrantă a strategiei, apreciindu-se că alinierea strategică dintre IT și obiectivele organizației reprezintă un factor critic de succes. Guvernanța IT asigură realizarea acestui factor critic de succes prin dezvoltarea eficientă și efectivă a securității, asigurarea informației corecte, precum și a tehnologiei aplicabile necesare.

Fundamental, guvernanța IT privește două aspecte:

- IT creează valoare pentru organizație, ca urmare a susținerii strategiei prin funcția IT;
- riscurile IT sunt cunoscute și monitorizate, urmărindu-se limitarea lor.

Guvernanţa IT este responsabilitatea consiliului de administraţie şi managementului executiv şi este parte integrantă a guvernanţei organizaţiei. Ea implică conducerea, structurile organizatorice şi procesele necesare, astfel încât funcţia IT să susţină strategia şi obiectivele organizaţiei.

Guvernanţa IT impune ca resursele sistemelor informaţionale să fie utilizate în convergenţă cu strategiile organizaţiei. Principiile care conduc guvernanţa IT se referă la:

- utilizarea mai eficientă şi cu riscuri minime a resurselor informaţionale;
- corelarea activităţii IT cu obiectivele strategice şi tactice ale organizaţiei.

Raportul Cadbury se concentrează asupra guvernanţei corporative şi recomandă deschiderea, integralitatea şi transparenţa mediului corporativ şi organizarea unui control adecvat şi eficient ca o componentă de bază a guvernanţei. În acelaşi timp, raportul face o referire directă la organizarea IT, arătând şi necesitatea existenţei unui control eficient al funcţionării acestuia. Raportul precizează că „guvernanţa IT este o responsabilitate a consiliului de administraţie şi a conducerii executive. Ea este o parte integrantă a guvernanţei organizaţiilor şi constă în atingerea obiectivelor sale strategice".

Principalele obiective ale guvernanţei IT sunt:

- alinierea activităţii IT la cerinţele de continuitate şi dezvoltare a afacerii;
- IT trebuie să genereze posibilitatea ca afacerea să îşi maximizeze profiturile;
- utilizarea cu responsabilitate a resurselor IT;
- managementul eficient al riscurilor legate de IT.

Din obiectivele enunţate se desprinde necesitatea ca funcţia IT să asigure creşterea automatizării proceselor afacerii şi asigurarea creşterii eficacităţii, reducerea costurilor şi asigurarea creşterii eficienţei şi mai buna administrare a riscurilor (securitate, credibilitate şi conformitate). Cadrul guvernanţei IT este reprezentat prin componentele sale, şi anume: definirea direcţiei de dezvoltare, stabilirea activităţilor IT, stabilirea obiectivelor, măsurarea performanţelor şi compararea performanţelor obţinute cu obiectivele fixate[1] (figura 2.1.1).

Funcţia IT a devenit critică pentru orice organizaţie deoarece ea susţine şi potenţează organizaţia. O guvernanţă IT eficace generează beneficii reale organizaţiei cum ar fi creşterea reputaţiei, încrederii, eficienţei conducerii, valorificarea oportunităţilor, reducerea costurilor, şi prin toate acestea, creşterea valorii pentru deţinătorii de interese.

[1] IT Governance Institute: *Board Briefing on IT Governance,* 2001, USA.

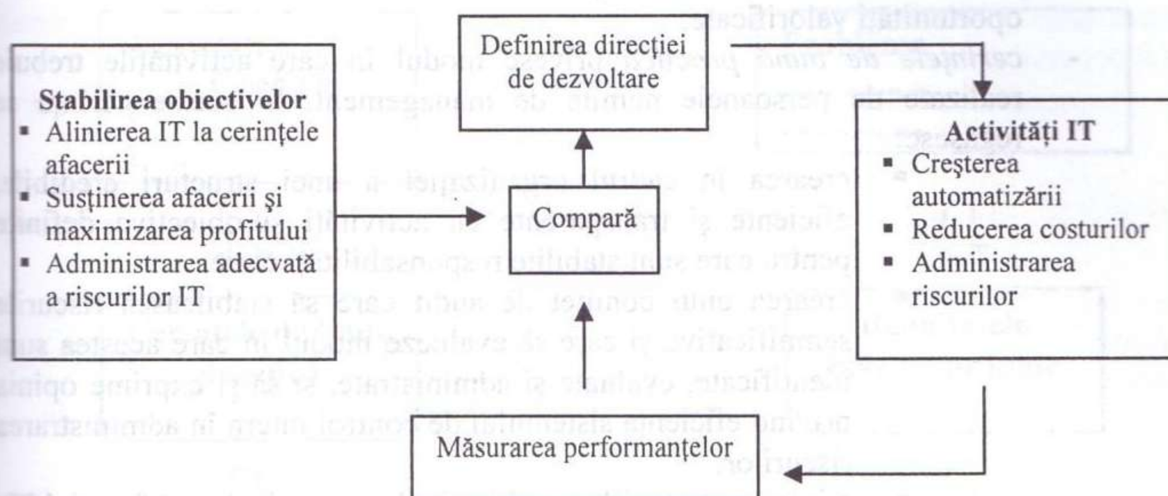


Figura 2.1.1. **Cadrul guvernanţei IT**

2.2. Reguli de bună practică pentru guvernanţa IT

Guvernanţa IT este o structură de relaţii şi procese folosită pentru a direcţiona şi controla organizaţia către atingerea obiectivelor, prin adăugarea de valoare asigurând echilibrul între riscurile şi beneficiile IT şi procesele sale. Folosirea tehnologiei informaţiei în toate aspectele economice şi eforturile sociale au creat o dependenţă de IT în iniţierea, înregistrarea, administrarea tuturor aspectelor privitoare la tranzacţiile economice, informaţii şi cunoaştere, creând un loc critic pentru guvernanţa IT în cadrul guvernanţei corporative.

Scopul guvernanţei corporative este de a dirija eforturile IT, astfel încât să se asigure performanţa IT necesară atingerii obiectivelor organizaţiei prin alinierea obiectivelor IT la acestea şi realizarea beneficiilor promise. În plus, IT trebuie să asigure organizaţiei exploatarea tuturor oportunităţilor şi maximizarea beneficiilor. Resursele IT trebuie să fie folosite responsabil, iar riscurile IT trebuie administrate adecvat.

Pentru a sigura implementarea unei guvernanţe IT eficiente este necesară întocmirea unor planuri care să vizeze următoarele elemente[2]:

- *o listă a activităţilor* pentru asignarea responsabilităţilor legate de guvernanţa IT şi problemelor ce trebuie să fie incluse în agenda guvernanţei IT;
- *rezultatele măsurilor* luate legate de problemele de guvernanţă IT cum ar fi alinierea obiectivelor de business şi respectiv IT, raportul cost-eficienţă

[2] Idem.

realizat de IT, capabilităţi şi competenţe generate, riscuri specifice, oportunităţi valorificate;

- *cerinţele de bună practică* privesc modul în care activităţile trebuie realizate de persoanele numite de management. În aceste cerinţe se regăsesc:
  - crearea în cadrul organizaţiei a unei structuri credibile, eficiente şi transparente cu activităţi şi obiective definite pentru care sunt stabilite responsabilităţi clare;
  - crearea unui comitet de audit care să stabilească riscurile semnificative şi care să evalueze modul în care acestea sunt identificate, evaluate şi administrate, şi să-şi exprime opinia privind eficienţa sistemului de control intern în administrarea riscurilor;
  - alinierea strategiilor şi obiectivelor organizaţiei şi funcţiei IT;
  - sporirea cunoştinţelor privind clienţii, produsele, piaţa şi procesele;
- *factorii critici de succes*. Aceştia reprezintă condiţii, competenţe şi atitudini critice pentru succesul organizaţiei. Aceşti factori sunt reprezentaţi de:
  - conştientizarea faptului că IT este parte integrantă a organizaţiei, şi nu doar o componentă răspunzătoare de probleme tehnice;
  - înţelegerea importanţei componentei IT şi asumarea responsabilităţilor de către management privitoare la acesta, solicitând şi sprijinul unor specialişti în domeniu;
  - crearea unei culturi organizaţionale care să încurajeze cooperarea interdepartamentală şi lucrul în echipă, să promoveze permanenta îmbunătăţire a proceselor şi să asigure o corectă abordare şi soluţionare a erorilor şi eşecurilor;
- *vectorii de performanţă* au rolul de a evidenţia modul în care guvernanţa IT este asigurată. De cele mai multe ori, ei sunt legaţi de factorii critici de succes şi se referă la următoarele aspecte:
  - extinderea şi frecvenţa riscurilor, precum şi modul de raportare către management;
  - îmbunătăţirea raportului cost-beneficii pentru procesele IT;
  - întreruperea funcţionării sistemelor;
  - timpul de răspuns al sistemelor.

Pentru a înţelege corelaţiile între elementele prezentate, propunem analiza următoarei reprezentări (figura 2.2.1):

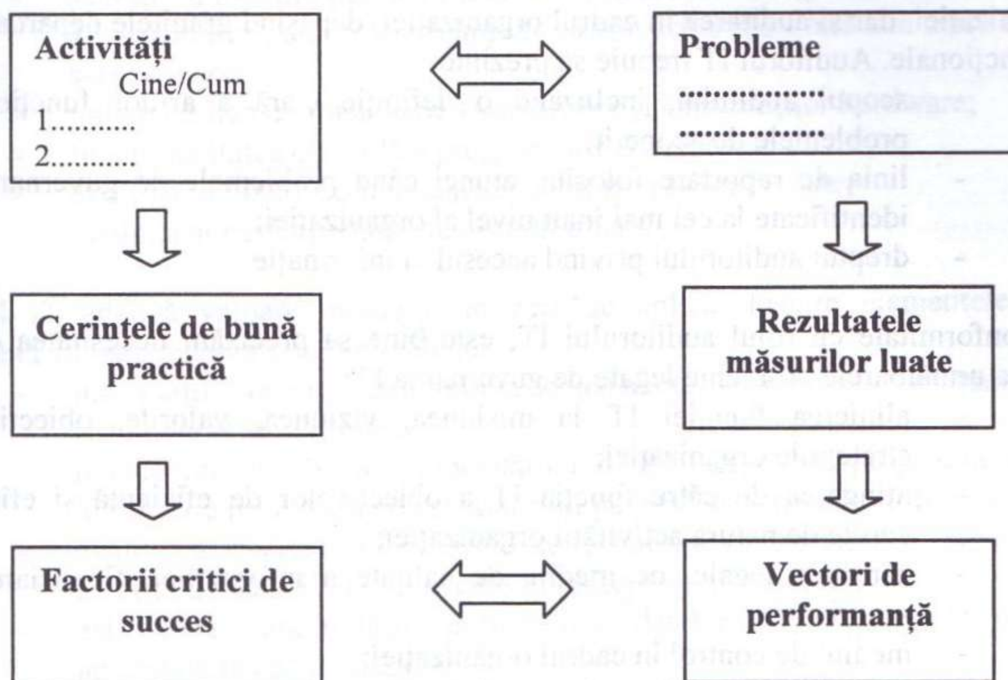


Figura 2.2.1. **Implementarea guvernanței IT**

Rolul auditului în guvernanța IT

Guvernanța IT, ca domeniu component al guvernanței organizației, vizează modul în care funcția IT este implementată funcționează în cadrul organizației. IT reprezintă astăzi o funcție intrinsecă, și nu o funcție marginală, separată de restul organizației. Astăzi, funcția IT își aduce aportul indiscutabil la realizarea obiectivelor organizației. Acest fapt determină necesitatea ca organizația să-și evalueze guvernanța IT, devenită o componentă tot mai importantă a guvernanței organizației.

Auditul joacă un rol deosebit de important în implementarea guvernanței IT în cadrul organizației. Auditul poate oferi senior-managementului recomandările necesare pentru îmbunătățirea calității și eficienței guvernanței IT.

Ca entitate chemată să asigure conformitatea, auditul ajută la asigurarea conformității în cazul proiectelor IT inițiate în cadrul organizației. Monitorizarea continuă, analiza și evaluarea metricilor asociați cu inițiativele guvernanței IT necesită o evaluare independentă care conduce la îmbunătățirea proceselor IT și inițiativelor guvernanței IT asociate.

Raportarea asupra guvernanţei IT implică auditarea la cel mai înalt nivel în cadrul organizaţiei, dar şi auditarea în cadrul organizaţiei, depăşind graniţele departamentale şi funcţionale. Auditorul IT trebuie să prezinte:

- scopul auditului, incluzând o definiţie clară a ariilor funcţionale şi problemele de acoperit;
- linia de raportare folosită, atunci când problemele de guvernanţă sunt identificate la cel mai înalt nivel al organizaţiei;
- dreptul auditorului privind accesul la informaţie.

În conformitate cu rolul auditorului IT, este bine să precizăm necesitatea de a se audita următoarele probleme legate de guvernanţa IT:

- alinierea funcţiei IT la misiunea, viziunea, valorile, obiectivele şi strategiile organizaţiei;
- atingerea de către funcţia IT a obiectivelor de eficienţă şi eficacitate cerute de natura activităţii organizaţiei;
- cerinţele legale, de mediu, de calitate a informaţiei, financiare şi de securitate;
- mediul de control în cadrul organizaţiei;
- riscurile inerente în cadrul mediului IT.

Funcţia IT este o funcţie dinamică, dependentă atât de evoluţia organizaţiei, cât şi de evoluţiile tehnologice specifice. În condiţiile existenţei unui mediu IT complex, structura principalelor controale interne se schimbă. În afara procedurilor de control şi a ariilor de control specifice activităţii organizaţiei, mediul IT impune o structură de control specifică ce se referă la:

- strategia şi planificarea resurselor informaţionale;
- implementarea şi gestionarea sistemului de aplicaţii;
- software-ul de bază;
- implementarea, exploatarea şi administrarea bazei de date;
- operaţiile şi procedurile specifice IT;
- securitatea IT.

Auditul IT este impus de evoluţiile spectaculoase în domeniul IT cum ar fi:

- aplicaţiile au din ce în ce mai multe controale încorporate, de aceea trebuie evaluată eficienţa acestora şi factorii de risc asociaţi;
- procedurile de prelucrare sunt din ce în ce mai automatizate şi integrate. O eroare poate afecta întreg lanţul de prelucrări;
- erorile umane pot conduce la consecinţe din ce în ce mai grave;
- managementul organizaţiilor, dar şi natura activităţilor desfăşurate impun cerinţe din ce în ce mai ridicate privind confidenţialitatea, disponibilitatea şi integritatea datelor;

- accesul la mediile publice (internet) impune tehnici speciale de detectare a intruziunilor, de protejare împotriva atacurilor din afară sub orice formă s-ar produce;
- îmbunătățirea continuă a performanțelor și capacităților hardware;
- funcționalitatea crescută a programelor de aplicații;
- evoluția în planul comunicațiilor și transferurilor de date;
- evoluția și perfecționarea factorului uman.

Auditul IT adaugă valoare mediului în care se aplică. Printre elementele care reprezintă valoare adăugată se pot include:

- informații corecte, disponibile, consistente și relevante asigurate de sistemele informaționale;
- înțelegerea mai bună a capacităților de prelucrare ale propriului sistem informatic prin evaluarea și controlul general al sistemului informatic;
- evaluarea corectă a nivelului de securitate a sistemului informatic, însoțită de măsuri eficiente care să protejeze informațiile;
- asigurarea continuității prelucrărilor datelor pe baza unor planuri aplicabile în caz de dezastre;
- recomandările ce însoțesc rapoartele de audit, recomandări ce potențează capacitățile de prelucrare ale sistemului.

2.3. Comitetul strategiei IT

Existența comitetului de strategie IT în cadrul organizației reprezintă implementarea regulilor de bună practică în cadrul organizației. Comitetul asigură asistență în stabilirea strategiilor, dar în egală măsură asistă bordul în îndeplinirea responsabilităților de guvernanță IT și își focalizează atenția asupra monitorizării riscurilor și performanței IT. Acesta este un mecanism de implementare a guvernanței IT în guvernanța organizației. Comitetul asistă bordul în modul în care acesta monitorizează problemele legate de IT asigurându-se că membrii acestuia dețin informațiile interne și externe necesare pentru luarea deciziilor necesare pentru o guvernanță IT eficientă.

În mod tradițional, organizațiile dispun de un comitet de coordonare (*steering committee)* la nivel executiv, care se ocupă de probleme IT importante pentru întreaga organizație. Subliniem necesitatea unei înțelegeri clare a ceea ce implică strategia IT și nivelurile de dirijare (steering). De aceea prezentăm viziunea CISA privind responsabilitățile și autoritatea celor două organisme (tabelul 2.3.1)[3].

[3] CISA Review Manual, 2006.

Tabelul 2.3.1. **Analiza responsabilităţilor Steering Committee**

Nivel	**Consiliul de administraţie**	**Nivel executiv**
Responsabilităţi	Oferă bordului recomandări pe teme privind: • relevanţa dezvoltărilor IT din perspectiva afacerii • alinierea IT la evoluţia afacerii • realizarea obiectivelor IT strategice • disponibilitatea resurselor IT necesare, pregătirea şi infrastructura necesară pentru îndeplinirea obiectivelor strategice • optimizarea costurilor IT, inclusiv rolul şi valoarea livrărilor provenite din outsourcing-ul IT • riscuri, recuperarea investiţiilor şi aspecte competitive legate de investiţiile IT • evoluţia proiectelor IT importante • contribuţia IT la derularea afacerii • expunerea la riscurile IT, inclusiv riscurile de conformitate • managementul riscurilor IT • îndrumarea managementului privind strategia IT • direcţii şi catalizatori pentru consiliul de administraţie privind practicile de guvernanţă IT	Decide asupra cheltuielilor IT şi a modului de alocare a costurilor: • aprobă arhitectura IT din cadrul organizaţiei • aprobă planurile proiectelor şi bugetele aferente, stabilind priorităţile • asigură şi alocă resursele necesare • urmăreşte ca proiectele să satisfacă cerinţele afacerii • monitorizează realizarea proiectelor în vederea obţinerii rezultatelor prevăzute şi încadrarea în bugete şi termene • monitorizează resursele şi conflictele privind priorităţile între diferitele direcţii şi funcţia IT şi între proiecte • face recomandări şi cereri pentru modificarea planurilor strategice (priorităţi, fonduri, abordări strategice, resurse etc.) • comunică echipelor de proiect obiectivele strategice • aduce o contribuţie majoră responsabilităţilor managementului privind guvernanţa IT
Autoritate	Îndrumă consiliul de administraţie şi managementul privind strategia IT: • este delegat de consiliul de administraţie să ofere	• Asistă conducerea executivă în elaborarea strategiei IT • Urmăreşte zilnic managementul serviciilor IT oferite şi proiectele IT

	intrările pentru strategie și să pregătească aprobarea acesteia • se concentrează pe probleme curente și de perspectivă privind strategia IT	• Urmărește probleme de implementare
Membrii	• Membrii ai consiliului de administrație și specialiști care nu fac parte din consiliul de administrație	• Utilizatori-cheie (executivi în linia de business) • CIO • Specialiști (IT, audit, juridic, financiar)

Standard it balanced scorecard

Standard it balanced scorecard reprezintă o tehnică de evaluare a procesului de management care poate fi aplicată procesului de guvernanță IT a afacerii în evaluarea funcțiilor și proceselor IT. Metoda depășește evaluarea financiară tradițională prin includerea evaluărilor privind satisfacția utilizatorilor, proceselor interne (operaționale) și capacitatea de inovare. Aceste evaluări tradiționale conduc organizația spre un optim al utilizării IT, aliniată obiectivelor strategice ale organizației. Pentru a putea fi aplicată funcției IT, se folosește o structură pe trei niveluri, urmărindu-se patru perspective:

- misiune, spre exemplu:
  - devenită principalul furnizor pentru sisteme informaționale;
  - oferirea de aplicații și servicii IT eficiente și eficace;
  - oferirea unei contribuții rezonabile a investițiilor IT asupra afacerii;
  - dezvoltarea de oportunități și răspunsul la provocări viitoare;
- strategii, spre exemplu:
  - dezvoltarea de aplicații și operațiuni superioare;
  - dezvoltarea de parteneriate între utilizatori și sporirea serviciilor oferite clienților;
  - oferirea de niveluri de servicii îmbunătățite și structuri de preț competitive;
  - controlul cheltuielilor IT;
  - dezvoltarea de noi capabilități pentru business;
  - pregătirea personalului IT și promovarea excelenței;
  - asigurarea susținerii pentru cercetare și dezvoltare;
- evaluări, spre exemplu: oferirea unui set de metrici pentru fundamentarea deciziilor IT.

Folosirea *Standard it balanced scorecard* reprezintă unul dintre cele mai eficiente mijloace de a sprijini comitetul de coordonare (*steering committe)* pe probleme IT şi managementul în realizarea alinierii IT cu businessul. Obiectivele vizează stabilirea modalităţii de raportare a managementului către consiliul de administraţie, asigurarea consensului între deţinătorii de interese în ceea ce priveşte problemele strategiei IT, demonstrarea eficienţei şi a valorii adăugate asigurate de IT precum şi comunicarea performanţelor IT, riscurilor şi capabilităţilor.

2.4. Guvernanţa securităţii informaţiei

În cadrul guvernanţei IT, o activitate deosebit de importantă este reprezentată de guvernanţa securităţii. Aceasta vizează: integritatea informaţiei, continuitatea serviciilor şi protecţia activelor. Urmare a existenţei şi utilizării pe scară largă a reţelelor globale şi extinderii organizaţiei în afara graniţelor ei tradiţionale, securitatea a devenit o temă extrem de importantă a guvernanţei IT.

Arhitectura organizaţiei

Un domeniu de interes sporit în cadrul guvernanţei IT este reprezentat de arhitectura organizaţiei. Arhitectura organizaţiei poate fi definită ca documentarea într-o manieră structurată a activelor IT ale organizaţiei în vederea facilitării înţelegerii, managementului şi planificării investiţiilor IT. În această abordare, ea implică atât reprezentarea stării curente, cât şi reprezentarea sării optimizate viitoare.

Concentrarea atenţiei pe arhitectura organizaţiei este urmarea creşterii complexităţii IT, a complexităţii organizaţiilor moderne şi a necesităţii alinierii funcţiei IT la strategia de afaceri astfel încât investiţiile în IT să asigure beneficiile dorite.

Fundamentele teoretice ale arhitecturii organizaţiilor au fost formulate de John Zachman la sfârşitul anilor '80, în viziunea sa sistemele IT putând fi realizate în aceeaşi manieră ca şi construirea unei case. Cadrul descris de Zachman este sintetizat în tabelul 2.4.1.

Tabelul 2.4.1. **Abordarea Zachman privind arhitectura întreprinderilor**

	Data	Funcțional (aplicație)	Rețea (tehnologie)	Oameni (organizare)	Procese (diagramă)	Strategie
Scop						
Modelul întreprinderii						
Modelul sistemelor						
Modelul tehnologiei						
Reprezentarea detaliată						

Completarea acestei matrice este destul de dificilă, multe organizații întâmpinând greutăți în completarea celulelor.

Arhitectura organizației dirijată de tehnologie urmărește să clarifice complexitatea alegerilor tehnologice în organizația modernă. Scopul este de a oferi îndrumare în ceea ce privește opțiunea organizației pentru utilizarea mediilor tehnice avansate și momentul aplicării acestora.

Arhitectura organizației dirijată de procese urmărește înțelegerea organizației în termeni de centru de creare a valorii adăugate și procese-suport. Se dorește înțelegerea proceselor, componentelor lor și a tehnologiei pe care acestea o necesită, îmbunătățirea activității fiind urmarea reproiectării și înlocuirii progresive a acestora. Baza acestei abordări este reprezentată de lanțul valorii, teorie formulată de Michael Porter în anii '80.

2.5. Strategia sistemelor informaționale

Planificarea strategică

Sub responsabilitatea managementului, se procedează la identificarea soluțiilor optime din punct de vedere al raportului cost-eficacitate vizând probleme și oportunități care privesc organizația și realizarea planurilor de acțiune pentru identificarea și asigurarea resurselor necesare. În realizarea planurilor strategice, acoperind de la trei la cinci ani, organizația trebuie să se asigure că aceste soluții IT se aliniază și respectă țelurile și obiectivele de ansamblu ale organizației.

Planificarea strategică a unei funcții IT eficiente implică luarea în considerare a cerințelor organizației privind componenta IT și capacitatea sa de aprovizionare pe această componentă. Determinarea cererii IT va implica o considerare sistematică a intențiilor strategice ale organizației, translatarea acestora în obiective specifice și

iniţiative de afaceri, estimarea capabilităţilor IT necesare pentru susţinerea acestor obiective şi iniţiative. În evaluarea capabilităţilor IT, portofoliul sistemelor existente va fi revizuit în ceea ce priveşte funcţionalitatea, costul şi riscurile. Planificarea aprovizionării IT implică evaluarea infrastructurii tehnice IT şi a proceselor suport principale, practicile de dezvoltare şi mentenanţă a software-ului, administrarea securităţii şi a serviciilor helpdesk, cu scopul de a determina dacă expansiunea sau îmbunătăţirea acestora este necesară.

Este important ca procesul de planificare strategică să aibă în vedere nu doar achiziţionarea de noi sisteme şi tehnologii, ci şi considerarea beneficiilor asigurate de aceste investiţii IT.

Auditorul SI va trebui să acorde toată atenţia planificării strategice IT, luând în considerare practicile de control ale managementului. Obiectivele de guvernanţă IT cer ca planurile de strategie IT să fie sincronizate cu celelalte strategii de afaceri. În aceste condiţii este important ca auditorul SI să se concentreze asupra proceselor de planificare strategică sau cadrul de planificare. O atenţie specială se va acorda translatării planurilor operaţionale sau tactice din planurile strategice, conţinutului planurilor strategice, cerinţelor de actualizare şi comunicare a planurilor, monitorizării şi evaluării cerinţelor.

Politici şi proceduri

Politicile şi procedurile reflectă modalitatea de dirijare asigurată de managementul în crearea de controale asupra sistemelor informaţionale şi resursele acestora.

Politici

Politicile reprezintă psihologia organizaţiei şi gândirea strategică a managementului superior, precum şi a deţinătorilor de procese de afaceri. Pentru a fi eficiente, politicile trebuie să fie eficiente şi clare. Responsabilitatea managementului este de a crea un mediu de control eficient, asumându-şi responsabilitatea de a formula, dezvolta, documenta, promulga şi controla politici acoperind ţelurile generale şi directivele[4]. În egală măsură managementul trebuie să se asigure că angajaţii cunosc şi înţeleg politicile aplicabile domeniului în care ei lucrează.

La nivelul departamentelor din structura organizatorică a organizaţiei se definesc propriile politici (sectoriale/departamentale), desprinse din politicile globale, vizând aspecte operaţionale. În general, abordarea top-down în definirea politicilor se dovedeşte mai eficientă, permiţând definirea politicilor sectoriale plecând de la

4 Idem.

politicile globale ale organizației. Există însă și posibilitatea opțiunii pentru abordarea bottom-up, caracteristică câștigurilor competitive.
Considerăm necesar să atenționăm asupra necesității revizuirii periodice a politicilor, această activitate fiind în responsabilitatea managementului. Nevoia revizuirii și actualizării lor periodice este determinată de implementarea noilor tehnologii și a modificărilor semnificative în procesele de afaceri, exploatând elemente de tehnologia informației și eficienței în planul productivității sau al câștigurilor competitive. Politicile trebuie să asigure realizarea obiectivelor de afaceri stabilite și implementarea celor mai adecvate controale asupra sistemelor.

Auditorul SI are obligația să cunoască și să înțeleagă aceste politici și să procedeze apoi la evaluarea conformității acestora.

Politica de securitate a informației

Politica de securitate comunică utilizatorilor, managementului și personalului tehnic, un standard de securitate coerent. Politica de securitate pentru informații și tehnologia specifică reprezintă primul pas către construirea unei infrastructuri de securitate. Politicile vor oferi informația privind instrumentele și procedurile necesare organizației. Ele trebuie să ofere un echilibru între nivelul de control și nivelul de productivitate, ceea ce înseamnă că suma costurilor legate de control nu trebuie să depășească beneficiile obținute. În proiectarea și implementarea acestor politici de securitate un rol extrem de important îl are cultura organizațională. Politica de securitate este supusă aprobării managementului superior și apoi trebuie documentată și comunicată tuturor angajaților și furnizorilor de servicii.

Politica de securitate reprezintă pentru auditorul SI un cadru de referință în diversele sale sarcini, iar evaluarea adecvării acestei politici este un obiectiv obligatoriu al auditorului SI.

Proceduri

Procedurile derivă din politicile elaborate și trebuie să corespundă spiritului acestora. Procedurile trebuie să fie scrise într-o manieră concisă și clară, pentru a fi ușor înțelese și aplicate. Procedurile documentează procesele de business (administrative și operaționale), precum și controalele pe care acestea le cuprind. Elaborarea procedurilor este în responsabilitatea managementului mediu.

În mod firesc, procedurile sunt mai dinamice decât politicile pentru care au fost elaborate, și aceasta datorită faptului că ele trebuie să reflecte modificările în procesele de afaceri și în mediul acestora. De aceea, revizuirea periodică a acestora este obligatorie. Auditorul va evalua procedurile urmărind adecvarea lor în raport cu politicile și procesele pentru care au fost elaborate și apoi va proceda la testarea

controalelor prevăzute de acestea la nivelul proceselor de afaceri. Testarea controalelor urmăreşte aprecierea adecvării şi eficienţei lor în raport cu procesele.

Considerăm necesar să atenţionăm asupra necesităţii cunoaşterii şi aplicării stricte a procedurilor aprobate. De aceea, o atenţie deosebită trebuie acordată automatizării stocării, distribuţiei şi managementului procedurilor IT. Intranetul organizaţiei poate să reprezinte o soluţie în acest sens.

2.6. Managementul riscului

Managementul riscului reprezintă procesul de identificare a vulnerabilităţilor şi ameninţărilor resurselor informaţionale utilizate de organizaţie în atingerea obiectivelor de business şi stabilirea contramăsurilor în vederea reducerii riscurilor la un nivel acceptabil, în raport cu valoarea resursei informaţionale pentru organizaţie.

Un management eficient al riscului începe cu înţelegerea clară a apetitului organizaţiei pentru risc. Acest apetit pentru risc, căruia îi corespunde un anume nivel al riscului acceptat, va determina toate eforturile de management al riscului în contextul IT, va afecta investiţiile viitoare în tehnologie, nivelul de protecţie a activelor şi nivelul poliţelor de asigurare necesare. Managementul riscurilor presupune identificarea, analiza, evaluarea, tratarea, monitorizarea şi comunicarea impactului riscului asupra proceselor IT. Fiind cunoscut apetitul pentru risc şi fiind identificate expunerile la risc, se pot stabili strategiile pentru managementul riscurilor şi clarificate apoi responsabilităţile. În funcţie de tipul riscului şi semnificaţia acestuia pentru business, managementul şi consiliul de administraţie pot decide asupra uneia dintre următoarele posibilităţi:

- evitarea riscului (opţiunea de a nu implementa anumite activităţi sau procese care pot induce riscuri mai mari);
- limitarea riscului, prin implementarea controalelor pentru a proteja infrastructura IT;
- transferul riscului, prin outsourcing, caz în care are loc partajarea riscului cu partenerii sau transferarea riscului către o firmă de asigurare;
- acceptarea, ceea ce înseamnă recunoaşterea existenţei riscului şi monitorizarea acestuia.
- eliminarea, atunci când este posibil, prin îndepărtarea sursei riscului.

Riscurile pot fi reduse prin implementarea sau îmbunătăţirea controalelor de securitate şi a procedurilor. Organizaţia poate decide să accepte riscurile atunci când costurile controalelor depăşesc beneficiile implementării controalelor.

Realizarea unui program de management al riscului

Realizarea unui program de management al riscului presupune:

- stabilirea scopului programului. Această etapă constă în determinarea scopului programului pentru managementul riscului. Scopul programului poate consta în reducerea costului asigurărilor sau reducerea numărului de stricăciuni. Plecând de la determinarea intenției, înaintea inițierii programului, organizația poate evalua rezultatele pentru a-i vedea eficiența. Responsabilitățile legate de realizarea planului de management al riscurilor revin directorului executiv și comitetului de direcție;
- stabilirea responsabilităților pentru planul de management al riscurilor. Această etapă presupune stabilirea unei echipe responsabile pentru dezvoltarea și implementarea planului. Dacă la început echipa este responsabilă pentru planul de management al riscului, nu trebuie uitat faptul că este absolut necesar să se procedeze la integrarea managementului riscului cu toate nivelurile din structura organizatorică. Personalul cu atribuții operaționale, precum și membrii consiliului de administrație, trebuie să asiste comitetul de management al riscurilor în identificarea riscurilor, realizarea controalelor și dezvoltarea strategiilor de intervenție.

Procesul de management al riscului

Punctul de plecare este reprezentat de identificarea și clasificarea resurselor informaționale sau activelor prezentând vulnerabilități. Scopul clasificării poate să fie prioritizarea investigațiilor viitoare și identificarea protecției adecvate (clasificarea bazată pe valoarea activelor) sau crearea posibilității de a utiliza un model standard de protecție (clasificarea în raport de caracterul critic și senzitivitatea resurselor informaționale). În categoria activelor asociate cu informații și IT cuprindem:

- informații și date;
- hardware;
- software;
- servicii;
- documente;
- personal.

Alte categorii de active care pot fi avute în vedere sunt reprezentate de: clădiri, stocuri, numerar, active intangibile, fondul comercial sau imaginea/reputația organizației.

Procesul continuă cu evaluarea amenințărilor și vulnerabilităților asociate cu resursele informaționale și a probabilității apariției lor.

Ameninţările se definesc drept circumstanţe sau evenimente cu potenţialul de a determina afectări ale resurselor informaţionale, cum ar fi distrugerea, divulgarea, modificarea datelor şi/sau refuzul serviciilor. Principalele categorii de ameninţări sunt reprezentate de:

- erori;
- distrugeri intenţionate/atacuri;
- fraude;
- furt;
- eşecul echipamentelor/software-ului.

Ameninţările apar ca urmare a vulnerabilităţilor asociate utilizării resurselor informaţionale. Vulnerabilităţile sunt reprezentate de caracteristicile resurselor informaţionale care pot fi exploatate de o ameninţare pentru a o afecta. Exemple de vulnerabilităţi identificate sunt reprezentate de:

- neştiinţa utilizatorilor;
- breşe în funcţionalitatea securităţii;
- parole alese neinspirat;
- tehnologie netestată;
- transmisii neprotejate în linia de comunicaţie.

Rezultatul oricăreia dintre aceste ameninţări se numeşte impact şi poate să se manifeste într-o pierdere de un fel sau altul. În cazul societăţilor comerciale, ameninţările conduc direct la pierderi financiare pe termen scurt sau la pierderi financiare indirecte pe termen lung. Putem exemplifica astfel de pierderi prin următoarele:

- pierderi financiare (numerar sau credit);
- încălcări ale legislaţiei;
- afectări ale reputaţiei/fondului comercial;
- punerea în pericol a angajaţilor sau clienţilor;
- afectarea încrederii;
- pierderea unor oportunităţi de afaceri;
- reducerea eficienţei operaţionale/performanţei;
- întreruperea activităţii.

Odată stabilite elementele de risc, ele se combină pentru a avea o imagine globală a riscurilor. O metodă de combinare a elementelor este cea prin care se calculează impactul vulnerabilităţii X (probabilitatea apariţiei privitoare la o anume resursă informaţională) pentru fiecare ameninţare, pentru a avea imaginea de ansamblu asupra riscului. Riscul este proporţional cu valoarea pierderii/distrugerii şi a frecvenţei estimate a ameninţării.

Odată riscurile identificate, se procedează la evaluarea controalelor existente sau la crearea de controale noi, cu scopul reducerii vulnerabilităţilor la un nivel acceptabil al

riscului. Controalele sunt considerate contramăsuri. Ele pot consta în acțiuni, dispozitive, proceduri sau tehnici. Puterea unui control poate fi măsurată prin eficiența lui și puterea conferită lui prin modul în care a fost proiectat. Elementele de control care trebuie luate în considerare în evaluarea puterii controlului au în vedere natura controlului – control preventiv sau detectiv, modalitatea lui de realizare – manual sau automat, modul de realizare – formalizat (prezentat în proceduri și urmărit prin evidențe cum este întreținut) sau ad hoc.

Riscul rezidual reprezintă nivelul estimat al riscului după aplicarea controlului. Riscul rezidual este utilizat de management pentru identificarea ariilor în care sunt necesare mai multe controale pentru reducerea în continuare a riscului. Apetitul managementului pentru risc este evidențiat prin nivelul de risc pe care acesta și-l asumă. Riscurile care depășesc acest nivel vor trebui în mod prioritar să fie diminuate prin introducerea unor noi controale. Riscurile aflate sub nivelul de risc acceptat trebuie, la rândul lor, evaluate pentru a se vedea dacă sunt supuse unor controale excesive. Este necesar de subliniat faptul că se pot obține diminuări ale costurilor prin reducerea controalelor excesive. Acceptarea riscurilor reziduale se face prin luarea în considere a următoarelor elemente:

- politica organizației;
- identificarea și măsurarea riscurilor;
- incertitudinea presupusă de evaluarea riscurilor;
- costul și eficiența implementării.

Este important să înțelegem că managementul riscului IT trebuie să opereze la mai multe niveluri, și anume:

- **nivelul operațional** – la acest nivel ne confruntăm cu riscuri care pot compromite eficiența sistemului IT și a infrastructurii-suport, posibilitatea de a ocoli sistemul de controale, pierderea sau indisponibilizarea unor resurse-cheie (sisteme, date, comunicații, personal, locații) și eșecul de a fi în conformitate cu legi și regulamente;
- **nivelul proiectului** – managementul riscului trebuie să aibă în vedere necesitatea înțelegerii și administrării complexității proiectului, în caz contrar existând riscul să nu se poată realiza toate obiectivele proiectului;
- **nivelul strategic** – este evaluată măsura în care funcția IT este aliniată la strategia de business, cum se plasează în raport de competitorii sau amenințările determinate de modificările tehnologice.

Identificarea, evaluarea și managementul riscurilor IT se realizează de persoane sau grupuri aparținând anumitor componente organizatorice din cadrul organizației. Însă aceste grupuri nu pot să lucreze separat deoarece un anumit risc afectează arii diferite. O disfuncționalitate majoră poate afecta disponibilitatea organizației de a oferi clienților serviciile convenite și poate avea implicații strategice, caz în care se impune implicarea managementului superior. În mod similar, probleme ale unui proiect

important pot avea implicaţii strategice. Cum multe proiecte oferă sisteme IT şi infrastructură noi, înseamnă că trebuie avut în vedere faptul că ele determină riscuri noi ale mediului IT.

Metode de analiză a riscurilor

În acest paragraf dorim să realizăm o prezentare sintetică a metodelor de management al riscurilor, şi anume metode calitative, semicalitative şi cantitative, precum şi prezentarea avantajelor şi dezavantajelor pe care acestea le prezintă.

Metode cantitative şi calitative

Metodele calitative folosesc cuvinte sau categorii descriptive pentru a exprima impactul sau probabilitatea. Sunt cele mai simple şi mai frecvent utilizate metode. Se bazează pe instrumente de lucru de tipul listelor de control şi clasificarea subiectivă a riscurilor pe o scară de tipul: mare, mediu, scăzut. Astfel de abordări nu dispun de rigoarea necesară pentru contabilitate şi management.

În **analizele semicantitative,** ratingurile descriptive sunt asociate cu scalele numerice. Aceste metode sunt folosite frecvent când nu este posibilă folosirea metodelor cantitative sau nu se poate reduce subiectivitatea în aplicarea metodelor calitative.

Analizele cantitative folosesc valori numerice pentru a descrie probabilitatea şi impactul riscurilor, folosind date din mai multe tipuri de surse cum ar fi înregistrările istorice, înregistrări şi practici folosite în diferite ramuri de activitate, teorii statistice, teste şi experimente. Multe analize cantitative de risc sunt folosite în mod curent în domeniul militar şi financiar. Următoarele secţiuni vor prezenta principalele concepte utilizate de metodele cantitative.

Probabilitate şi expectaţie

Majoritatea acestor metode sunt bazate pe teorii statistice „clasice" ale probabilităţii şi expectaţiei. Majoritatea fenomenelor naturale sunt afectate de multe variabile de aceea, numai în cazul determinării unor legi statistice pentru comportamentul lor, manifestările lor actuale pot să fie apropiate valorilor anticipate în baza acestor determinări. Variabilele cum ar fi cele sociale, economice şi tehnologice sunt subiectul unui comportament stocastic. Apariţia unei furtuni nu poate fi prezisă cu acurateţe, dar, dacă există suficientă informaţie istorică pentru definirea unui trend, probabilitatea apariţiei ei poate fi făcută cu o anume acurateţe.

Dacă probabilitatea unui eveniment **p** este stabilită (0 =< **p** <= 1) și este cunoscută valoarea unui activ (**v**), afectat de respectivul eveniment, atunci pierderea (sau câștigul) este dată de expresia **v x p.**

Metoda expectației pierderii anuale

Expectația pierderii anuale (*annual loss expectation* – **ALE**) simplifică asignarea valorii (**v**) la probabilitatea (**p**) într-o manieră mai ușor de determinat. Se procedează la crearea unui tablou, prin intermediul unui worksheet, dezvoltat pe două coordonate: materialitate și orizont de timp. Pierderea anuală anticipată va fi determinată pentru frecvențe de apariție ale evenimentului și se descrie pe o scală de tipul: un minut, o oră, o zi, o săptămână, ..., un an, cinci ani, zece ani, ..., 100 de ani etc. Valoarea bunurilor (exprimată în mii unități monetare) se dezvoltă pe o scară de tipul: 1, 100, 1000, 10.000, 100.000, 1 mil, ... 1 mld., valoarea anualizată a pierderii fiind citită la intersecția liniei și coloanei aferente frecvenței anticipate a evenimentului și respectiv a valorii estimate a bunului.

Apreciem că este bine de subliniat faptul că managementul de risc bazat pe metode cantitative este preferabil abordărilor calitative. Metodele cantitative oferă estimări mai obiective. Managementul va trebui să acorde atenția cuvenită evenimentelor pentru care s-a estimat un impact mare chiar dacă frecvența de apariție estimată este foarte mică. Determinarea probabilităților viitoare pe date istorice este adesea dificilă. Atunci când evenimentele nu au precedent, este precaut să se ia în considerare cazul cel mai pesimist.

2.7. Practici de management al sistemelor informaționale

Practicile de management al sistemelor informaționale reflectă implementarea politicilor și procedurilor dezvoltate pentru diferitele SI. În majoritatea organizațiilor, Departamentul IT este o structură-suport menită să servească departamentele de producție în desfășurarea operațiilor lor curente în condiții de eficiență și eficacitate. Astăzi, sistemele informaționale au devenit o parte integrantă a oricărei activități desfășurate în cadrul organizației. Având în vedere această caracteristică, precum și faptul că importanța SI crește permanent, auditorul SI trebuie să înțeleagă și să aprecieze nivelul la care managementul SI asigură atingerea obiectivelor organizației. Revizuirea politicii/procedurilor legate de activitatea departamentului IT include practicile de management al resursei de personal, sursa și managementul schimbării IT.

Managementul resursei de personal

Managementul resursei de personal vizează politicile și procedurile de angajare, promovare, menținere și pensionare.

Procedurile de angajare permit selecţia personalului astfel încât să se asigure alegerea celui mai eficient şi bine pregătit personal, iar procesul de angajare se derulează în conformitate cu reglementările legale de recrutare. Controalele principale pentru procesul de angajare sunt reprezentate de:

- verificări ale pregătirii;
- angajamente de confidenţialitate;
- încheierea de asigurări, acolo unde legislaţia permite acest lucru în vederea protejării organizaţiei pentru riscul de fraudă, furt, greşeli sau neglijenţa angajaţilor;
- angajamente privind conflictul de interese;
- angajamente de nonconcurenţă.

Ghidurile angajaţilor, distribuite tuturor angajaţilor, prezintă prevederi privind:

- politicile şi procedurile de securitate;
- expectaţiile organizaţiei;
- beneficiile angajaţilor;
- politica de concedii;
- reguli privind orele suplimentare;
- evaluarea performanţelor;
- proceduri de urgenţă;
- acţiuni disciplinare.

Organizaţia trebuie să deţină un cod de etică, disponibil tuturor angajaţilor care să prezinte detaliat şi clar responsabilităţile acestora şi principiile care reglementează conduita acestora.

Politicile de promovare

Politicile de promovare trebuie să fie corecte, cunoscute şi înţelese de toţi angajaţii. Ele trebuie să se bazeze pe criterii obiective, să ia în considerare performanţa individuală a angajaţilor, nivelul de instruire, experienţa şi nivelul de responsabilitate.

Auditorul SI trebuie să se asigure că există la nivelul SI politici şi proceduri pentru promovare.

Pregătirea continuă

Pregătirea continuă a angajaţilor şi în mod special a specialiştilor IT, confruntaţi cu schimbări rapide în planul tehnologiei şi produselor software, este necesar să se desfăşoare în mod organizat. Pregătirea trebuie realizată ori de câte ori se procedează la achiziţionarea de noi echipamente sau componente software. În egală măsură este necesar să se acorde atenţia cuvenită instruirilor având ca temă managementul proiectelor.

Practici în asigurarea resurselor IT

Strategia de asigurare a resurselor IT se stabilește pentru fiecare componentă pentru a se identifica abordarea care asigură cel mai bine realizarea obiectivelor stabilite la nivelul organizației. Practicile utilizate în scopul asigurării resurselor funcțiilor IT sunt:

- prin efort propriu (*insourced* sau *in-house*): organizația optează pentru asigurarea funcțiilor IT prin personal propriu;
- externalizarea (*outsourcing*): procurarea facilităților se realizează de la furnizori specializați;
- abordarea mixtă presupune asigurarea funcțiilor IT atât cu personal propriu, cât și prin firme specializate.

Dacă se dorește clasificarea în funcție de locația din care este asigurată funcția IT, se poate proceda la lucrul:

- onsite: personalul departamentului IT își desfășoară activitatea la sediul organizației;
- offsite: personalul departamentului IT își desfășoară activitatea într-o altă locație decât sediul organizației, dar în aceeași arie geografică;
- offshore: personalul departamentului IT își desfășoară activitatea într-o locație diferită de a organizației într-o zonă geografică diferită.

Stabilirea opțiunii pentru una sau alta dintre abordările posibile se realizează prin luarea în considerare a următorilor factori:

- este sau nu o funcție de bază;
- funcția analizată necesită cunoștințe speciale, procese și personal critice pentru realizarea obiectivelor organizației;
- funcția poate fi asigurată și de un terț sau dintr-o altă locație cu aceleași prețuri sau prețuri mai mici, cu aceeași calitate sau în condiții de calitate superioară și fără creșterea riscurilor;
- organizația dispune sau nu de experiența necesară pentru lucrul cu terți sau pentru derularea activităților SI și businessului din locații de tip offsite sau offshore.

Strategia de asigurare a funcției IT este evaluată și aprobată de comitetul IT. În cazul opțiunii pentru externalizare se va proceda la:

- definirea funcției IT care se va externaliza;
- stabilirea nivelului serviciilor necesare și nivelul minim al metricilor pentru evaluarea serviciilor;
- alegerea furnizorului;
- compararea costului soluției in-house cu prețul cerut de furnizor. Pot fi realizate analize mai detaliate pentru a se vedea dacă apelarea la un furnizor permite atingerea obiectivelor organizației la costuri mai mici cu riscuri limitate.

Acelaşi proces de analiză trebuie să se realizeze pentru cazul în care organizaţia optează pentru realizarea offshore a funcţiilor IT.

Strategii şi practici de outsourcing

Outsourcing-ul reprezintă o strategie prin care o organizaţie încredinţează funcţionalităţi majore unor furnizori externi, specializaţi în anumite servicii, care devin parteneri furnizori de servicii cu valoare adăugată. Majoritatea managerilor IT consideră outsourcing-ul drept cea mai bună soluţie pentru organizaţie de a eficientiza utilizarea resurselor prin reducerea costurilor şi accesul la tehnologii de ultimă oră.

Practica de outsourcing presupune încheierea de contracte cu furnizorii de resurse IT, fapt ce impune definirea în cadrul organizaţiei a procesului de outsourcing cu scopul administrării mai bune a relaţiei contractuale cu furnizorul. Furnizorul oferă resurse sau expertiza necesară pentru prestarea unui anumit serviciu. Outsourcing-ul a devenit pentru organizaţii nu doar o opţiune posibilă, ci chiar o necesitate. Auditorul SI trebuie să cunoască diferitele forme de outsourcing şi riscurile implicate de acestea.

Obiectivele specifice pentru externalizarea IT diferă de la o organizaţie la alta. Decizia de a asigura prin externalizare servicii şi/sau produse impune managementului să reevalueze controalele pe care se bazează.

Motivele alegerii externalizării includ:
- dorinţa de a se concentra pe activităţi de bază pentru organizaţie;
- presiunea pe marja de profit;
- nevoia de reducere a costurilor impusă de creşterea concurenţei;
- flexibilitate pentru organizaţie şi structura acesteia.

Pot fi externalizate următoarele servicii:
- introducerea datelor;
- proiectarea şi realizarea de noi sisteme informatice sau aplicaţii atunci când personalul organizaţiei nu dispune de cunoştinţele şi experienţa necesare sau este deja implicat în realizarea unor altor proiecte;
- mentenanţa aplicaţiilor existente pentru a permite personalului organizaţiei să dezvolte noi aplicaţii;
- operarea helpdesk-ului sau call-center-ului;
- realizarea unor prelucrări.

Avantajele outsourcing-ului sunt reprezentate de:
- realizarea de economii prin utilizarea de componente software reutilizabile;
- apelând la soluţiile oferite de firme specializate, organizaţiile pot accesa soluţii viabile, la înalte standarde de calitate şi securitate, rezultate din efortul investiţional al outsourcer-ului;

- furnizorii de resurse pot aloca mai mult timp și pot să lucreze concertat pe anumite proiecte, lucru greu de realizat prin resursele proprii ale organizației;
- furnizorii dispun de expertiza necesară în domenii tehnologice de vârf, expertiză de care organizația nu dispune;
- outsourcing-ul oferă în continuare organizației controlul asupra activităților/proceselor externalizate;
- outsourcing-ul reprezintă și o modalitate de partajare a riscurilor.

Organizația poate opta pentru una dintre următoarele variante de outsourcing:

- **outsourcing tactic**: relație contractuală destinată să acopere o problemă specifică sau pentru desfășurarea în timp a unor servicii dintr-o anumită arie funcțională (de exemplu, contract pentru dezvoltarea unor aplicații software specifice);
- **outsourcing strategic:** este reprezentat de o relație de lungă durată (cinci-zece ani) determinată de nevoia organizației de a se focaliza pe propriile competențe majore și de a externaliza restul activităților. În această categorie putem include: serviciile de business continuity, asigurarea și întreținerea infrastructurii hardware, partea de software, asigurând integrarea corectă și buna funcționare a diverselor componente;
- **transformational outsourcing:** de această dată, relația de externalizare nu este privită ca un mijloc de a crește eficiența, ci ca un factor care dirijează schimbarea, influențând direct businessul organizației.

Outsourcing-ul prezintă și unele dezavantaje, dintre care amintim:

- costurile pot depăși nivelul anticipat;
- pierderea experienței personalului SI ca urmare a faptului că nu mai continuă documentarea în domeniul ce face obiectul externalizării;
- posibilul eșec al furnizorului;
- accesul limitat la produs (ex.: în cazul achiziționării de software, clientul nu poate proceda la modificări ale acestuia);
- dificultățile în modificarea contractului semnat;
- posibilitatea neîndeplinirii prevederilor contractuale;
- posibila lipsă de loialitate a angajaților firmei contractante față de client;
- costurile serviciilor pot să nu rămână competitive pe toată durata contractului;
- afectarea reputației companiei ca urmare a eșecului proiectului etc.

Există însă și mijloace pentru limitarea acestor riscuri:

- stabilirea unor parteneriate care să permită realizarea unor obiective comune;
- utilizarea mai multor furnizori;
- realizarea periodică de reevaluări și analize de benchmarking;
- încheierea de contracte pe termen scurt;
- crearea unor echipe de management al contractului, formate din membrii asigurând responsabilități în cadrul unor funcții diferite în cadrul organizației;
- includerea în contracte a unor prevederi privind evenimente/probleme care pot fi anticipate.

Outsourcing-ul impune un management al relaţiei cu furnizorul de servicii. Contractul de outsourcing trebuie să includă descrierea mijloacelor, metodelor, proceselor şi structura care însoţeşte oferta de servicii şi produse SI, dar şi elementele de control al calităţii.

Auditorul SI are sarcina de a evalua periodic conţinutul contractelor de outsourcing şi nivelul serviciilor pentru a estima măsura în care sunt respectate prevederile contractuale. În egală măsură, auditorul poate proceda la evaluarea procedurilor outsourcer-ului şi rezultatele evaluărilor realizate de acesta prin programul de calitate care poate include metodologiile CMM şi ISO. Programele de calitate necesită desfăşurarea cu regularitate de misiuni de audit pentru a certifica procesul şi procedurile care îndeplinesc standardul de calitate.

Outsourcing-ul nu este urmarea unei decizii determinată de costul asigurării resursei SI, ci este o decizie strategică având implicaţii semnificative pentru management. Calitatea serviciilor, garantarea continuităţii serviciilor, controlul procedurilor, avantajul competitiv şi cunoştinţele tehnice sunt probleme în raport cu care are loc fundamentarea deciziei de externalizare. Este extrem de important să se aleagă cel mai potrivit furnizor, mai ales în cazul externalizării pe termen lung.

2.8. Structura organizatorică a SI şi responsabilităţi

Conform CISA, organigrama departamentului IT este cea prezentată în figura 2.8.1. Din analiza organigramei rezultă existenţa unor funcţiuni specializate pe probleme de securitate, dezvoltarea de aplicaţii şi mentenanţă, suport tehnic pentru reţea şi administrarea sistemului şi operaţii. Departamentul este condus de un director, iar în cazul companiilor mari, de un CIO (*chief information officer*).

Auditorul SI trebuie să stabilească printre obiectivele misiunii de audit şi evaluarea structurii organizatorice a departamentului IT, precum şi atribuţiile şi responsabilităţile înscrise în fişele posturilor. Auditorul va trebui să verifice măsura în care sunt respectate în activitatea curentă atribuţiile stabilite în fişele posturilor. Stabilirea atribuţiilor şi responsabilităţilor pe posturi, cu respectarea funcţiilor incompatibile, domeniul IT prezentând cerinţe specifice legate de acest aspect. Auditorul va trebui să analizeze următoarele funcţiuni:

- **managerii dezvoltării de sisteme**, responsabili cu programatorii şi analiştii care implementează sisteme noi dar care şi întreţin sistemele existente;
- **help desk** – reprezintă o entitate în cadrul organizaţiei, creată cu scopul de a răspunde întrebărilor tehnice şi problemelor utilizatorilor finali. Activitatea help desk-ului poate fi susţinută prin utilizarea de software achiziţionat de la firme de software. Procedura implementată la nivelul help desk-ului impune înregistrarea problemelor comunicate de utilizatorii finali ai sistemului informatic şi modul de soluţionare, informaţii necesare în analiza problemelor IT.

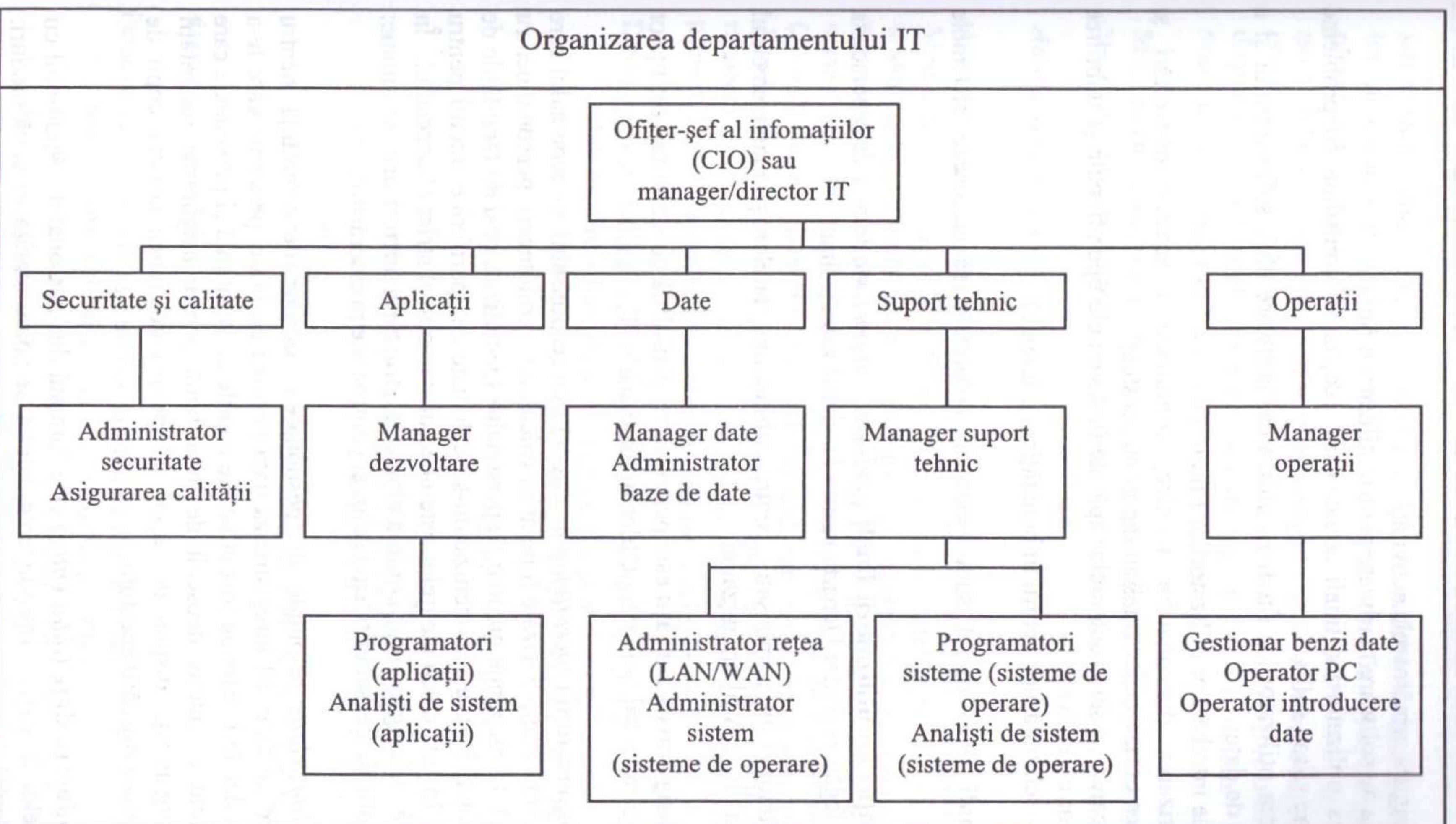


Figura 2.8.1. **Organizarea departamentului IT**

Help desk-ul asigură următoarele activităţi:
- achiziţia de software/hardware pentru utilizatorii finali;
- asistarea utilizatorilor finali atunci când aceştia se confruntă cu probleme hardware şi/sau software;
- pregătirea utilizatorilor finali în utilizarea hardware-ului, software-ului şi a bazelor de date;
- răspunde întrebărilor utilizatorilor finali;
- monitorizarea dezvoltărilor tehnice, comunicarea acestor dezvoltări şi instruirea utilizatorilor finali în raport cu acestea;
- identificarea sursei problemelor apărute în sistemele operaţionale şi stabilirea măsurilor corective;
- iniţierea schimbărilor pentru îmbunătăţirea eficienţei.

Utilizatorii finali (*end useri*) sunt persoane autorizate să acceseze sistemele operaţionale.

Managerul relaţiei cu utilizatorii finali (*end-user support manager*) este persoana responsabilă cu legătura dintre Departamentul IT şi utilizatorii finali.

Managerul datelor este responsabil pentru arhitectura datelor şi managementul datelor văzute ca un activ al organizaţiei.

Managerul cu asigurarea calităţii este persoana responsabilă cu stabilirea cerinţelor de calitate şi asigurarea calităţii activităţilor în toate ariile IT.

Managerul de operaţiuni (*operational manager*) este responsabil cu personalul care realizează operaţiuni computerizate (operatori calculator, bibliotecari, personal pentru controlul datelor). El răspunde nu doar de personalul specializat, ci şi de facilităţile de procesare automată, în acestea incluzându-se calculatoare, periferice, medii pentru stocarea datelor. În sala calculatoarelor este necesar un control strict al accesului. În această activitate, managementul controalelor este structurat în trei arii, şi anume: controlul securităţii fizice, securitatea datelor şi controalele prelucrărilor.

Bibliotecarul (*librarian*) răspunde de gestionarea copiilor de siguranţă pentru aplicaţii şi fişiere de date. El înregistrează data primirii copiilor, persoana care le-a depus, precum şi datele la care au fost eliberate copiile de siguranţă şi persoanele care le-au ridicat. Fiind o funcţie deosebit de importantă pentru asigurarea securităţii datelor, multe organizaţii dispun de suport IT pentru gestiunea acestor copii de siguranţă şi gestiunea mişcării acestora.

Echipa de introducere date (*data entry*) este formată din personalul responsabil cu introducerea datelor în sistem. Introducerea datelor se poate realiza în două moduri: introducere pe loturi (*batch*) sau introducere on-line. Metoda pe loturi presupune

introducerea unor seturi de documente, datele astfel introduse în sistem formând un lot, procesarea urmând a se realiza la nivelul acestuia. Metoda introducerii on-line presupune procesarea datelor pe măsura introducerii lor în sistem. Practica generalizării sistemelor distribuite a condus la realizarea introducerii datelor în mod on-line de către utilizatorii finali, ceea ce impune ca aplicațiile utilizate de aceştia să dispună de controalele necesare validării şi autorizării datelor. În acest context, necesitatea echipelor de data entry s-a redus simţitor.

Managerul suportului tehnic (*technical support manger*) este responsabil cu activitatea programatorilor de aplicații antrenați în întreținerea sistemului software.

Administrarea securității

Administrarea securității reprezintă o activitate necesară şi extrem de complexă. Modul în care ea se desfăşoară este urmarea înțelegerii de către managementul organizației a importanței evaluării şi controlului riscurilor. Managementul organizației aprobă politicile de securitate care stabilesc standardele şi procedurile de urmat. Cel care stabileşte politica de securitate este **administratorul securității** (*security administrator*). El este subordonat direct managerului de operațiuni. Administratorul securității are responsabilitatea de a asigura faptul că toți utilizatorii respectă politica de securitate, iar controalele existente sunt adecvate pentru a se preveni accesul neautorizat la date, programe şi echipament.

Dintre responsabilitățile administratorului securității amintim:

- stabilirea regulilor de acces la date şi alte resurse IT;
- asigurarea securității şi confidențialității asupra ID-urilor şi parolelor utilizatorilor;
- monitorizarea tentativelor de violare a securității şi luarea măsurilor corective;
- revizuirea şi evaluarea periodică a politicii de securitate prezentând managementului propuneri privind modificările necesare;
- pregătirea şi desfăşurarea programului de instruire a utilizatorilor în probleme de securitate;
- testarea securității arhitecturii sistemului în vederea identificării posibilelor amenințări.

Asigurarea calității

Personalul implicat în asigurarea calității desfăşoară două tipuri de activități:

- **asigurarea calității** (*quality assurance –QA*): ajută departamentul IT să asigure aplicarea corectă a proceselor, cu alte cuvinte programele şi documentațiile sunt în conformitate cu standardele stabilite;

- **controlul calităţii** (*quality control - QCI*) activitate care urmăreşte realizarea testelor pentru asigurarea faptului că aplicaţiile rulează corect şi răspund cerinţelor utilizatorilor. Controlul calităţii se desfăşoară la nivelul diferitelor stadii în dezvoltarea aplicaţiilor, dar în mod obligatoriu se realizează înaintea trecerii aplicaţiilor în utilizarea curentă.

Echipa de asigurare a calităţii răspunde de dezvoltarea, promulgarea şi întreţinerea standardelor pentru funcţia IT; organizează pregătirea continuă privind standardele şi procedurile; procedează la verificarea periodică a acurateţei şi autenticităţii intrărilor, procesării şi ieşirilor diferitelor aplicaţii. Pentru a putea să-şi îndeplinească responsabilităţile, acest grup trebuie să fie independent. Uneori el este inclus în grupul de control.

Administrarea bazei de date

Administratorul bazei de date (DBA) are responsabilitatea de a defini şi menţine structurile de date. Pentru a reuşi acest lucru, el trebuie să înţeleagă cerinţele organizaţiei şi utilizatorilor, precum şi relaţiile dintre date. Prin această poziţie administratorul răspunde de securitatea datelor partajate în cadrul sistemului şi de întreţinerea bazei de date. Administratorul bazei de date raportează direct managerului de operaţiuni.

În sinteză, responsabilităţile administratorului bazei de date sunt[5]:
- specificarea definiţiei fizice a datelor;
- modificarea structurii fizice a datelor pentru îmbunătăţirea performanţelor;
- selectarea şi implementarea instrumentelor de optimizare a bazei de date;
- testarea şi evaluarea programatorilor şi instrumentelor de optimizare;
- răspunde la întrebările programatorilor şi îi instruieşte pe aceştia cu privire la structurile bazei de date;
- implementarea definiţiei controalelor bazei de date, a controalelor accesului, controalelor actualizărilor şi controalelor accesului concurent;
- monitorizarea utilizării bazei de date şi a indicatorilor statistici referitori la performanţele bazei de date.

Administratorul bazei de date dispune de instrumentele necesare pentru stabilirea controalelor bazei de date şi are accesul la toate datele.

Departamentul IT asigură un control atent asupra administrării bazei de date prin:
- segregarea atribuţiilor;
- aprobarea de către management a activităţilor administratorului bazei de date;
- verificarea jurnalelor de control al accesului şi activităţilor;
- controale detective asupra utilizării instrumentelor bazei de date.

[5] Conform CISA.

Analiza sistemelor

Analiştii de sistem sunt specialişti cu atribuţii în proiectarea sistemelor în funcţie de nevoile utilizatorilor, de aceea ei sunt implicaţi mai ales în partea de început a ciclului de viaţă (SDLC). Ei analizează nevoile utilizatorilor şi dezvoltă specificaţii funcţionale şi ale datelor, asigurând şi proiectarea celor mai importante documente care vor permite programatorilor să realizeze aplicaţiile.

Arhitectura securităţii

Arhitecţii securităţii au rolul de a evalua tehnologiile de securitate. De aceea ei procedează la proiectarea aspectelor de securitate ale tipologiei reţelei, controlul accesului, precum şi a altor aspecte de securitate, finalizând prin definirea cerinţelor şi politicilor de securitate.

Dezvoltarea şi întreţinerea aplicaţiilor

Personalul specializat pe aplicaţii este responsabil cu dezvoltarea şi întreţinerea aplicaţiilor. Dezvoltarea presupune atât scrierea de programe noi, cât şi modificarea aplicaţiilor existente, inclusiv configuraţia aplicaţiilor. Pentru a exista un control al modificărilor realizate asupra aplicaţiilor, control asigurat de management, programatorii vor lucra **numai** într-un mediu de testare. Introducerea în utilizarea curentă a aplicaţiilor modificate se va realiza sub un control strict şi numai după autorizarea acestei operaţiuni de către persoanele autorizate în acest sens.

Dezvoltarea şi întreţinerea infrastructurii

Personalul responsabil cu infrastructura are ca rol întreţinerea sistemelor software, inclusiv a sistemului de operare. Aceste responsabilităţi pot impune accesul la întregul sistem. Managementul SI trebuie să monitorizeze foarte atent activităţile desfăşurate de aceştia prin verificarea jurnalelor electronice care reţin informaţii referitoare la activitatea lor, fără a exista posibilitatea alterării informaţiei înregistrate în aceste fişiere. Personalul responsabil cu infrastructura trebuie să aibă acces doar la bibliotecile de sistem unde se păstrează software-ul pe care ei trebuie să-l întreţină.

Managementul reţelei

Astăzi, numeroase organizaţii dispun de facilităţi de procesare dispersate. Chiar dacă dispun de facilităţi centrale de procesare, ele utilizează totodată:

- LAN – reţele locale la nivelul sucursalelor şi locaţii la distanţă;
- WAN – reţele pe arii extinse, la care reţelele locale pot fi interconectate pentru a facilita accesul unor utilizatori aflaţi în diferite locaţii;
- reţele de comunicaţii wireless – realizate cu ajutorul PDA-urilor (*Personal Digital Assistants*) sau alte dispozitive mobile.

Administratorii reţelelor sunt responsabili cu componentele-cheie ale acestei infrastructuri: routere, firewals, segmentarea reţelei, managementul performanţei,

accesul la distanţă etc. Datorită dispersiei geografice, fiecare reţea locală poate avea nevoie de un administrator. În funcţie de politica implementată în cadrul organizaţiei, ei pot raporta direct directorului cu facilităţile de procesare (IPF) sau managerului utilizatorului final. Administratorii de reţea răspund pentru controlul tehnic şi administrativ asupra reţelei locale, aceasta presupunând asigurarea funcţionării link-urilor necesare transmisiilor, backup-ul sistemului, asigurarea achiziţionării autorizate de software şi hardware. În cazul reţelelor mici, administratorii răspund şi de administrarea securităţii LAN. Segregarea responsabilităţilor impune ca administratorul de reţea să nu aibă responsabilităţi legate de programele de aplicaţii, dar poate avea responsabilităţi legate de programarea sistemelor şi utilizatorii finali.

2.9. Segregarea atribuţiilor în cadrul SI

Structura organizatorică şi denumirile posturilor pot diferi foarte mult de la o organizaţie la alta, în funcţie de dimensiunea şi natura activităţii. Pentru auditorul SI care va trebui să evalueze nivelul de segregare a atribuţiilor este extrem de important să obţină informaţii privind relaţiile dintre diferitele posturi, responsabilităţi şi autorităţi. Segregarea atribuţiilor evită posibilitatea ca o singură persoană să răspundă de diferite funcţii critice, astfel încât erori sau disfuncţionalităţi să apară fără a fi detectate la timp. Prin respectarea segregării atribuţiunilor se asigură descurajarea şi prevenirea atacurilor frauduloase şi actelor răuvoitoare. De aceea este foarte important să se asigure segregarea:
- custodiei activelor;
- autorizării;
- înregistrării tranzacţiilor.

Dacă nu se realizează o corectă segregare a atribuţiilor există riscul:
- deturnării activelor;
- întocmirii de situaţii financiare eronate;
- obţinerii unor documentaţii financiare deficiente;
- folosirii improprii a fondurilor sau al nedetectării unor modificări de date.

În condiţiile în care segregarea atribuţiilor este realizată corect, potenţialul distrugerilor cauzate de acţiunile unei persoane sunt limitate. Departamentul SI şi departamentele utilizatorilor finali trebuie să fie astfel organizate încât să existe o segregare adecvată a atribuţiilor (tabelul 2.8.1).

Controalele de compensare sunt controale interne introduse pentru a reduce riscul existenţei sau a unei potente slăbiri a controlului atunci când segregarea atribuţiilor nu poate fi făcută adecvat. În această situaţie se vor avea în vedere structura organizatorică şi rolurile pentru a se determina cele mai adecvate controale pentru mediul respectiv. Atunci când departamentul IT este mic, anumite combinaţii de responsabilităţi nu trebuie să se realizeze. Când acest lucru nu se poate realiza vor trebui introduse controale speciale.

Tabelul 2.8.1. **Controlul segregării atribuțiilor**

Matricea de control pentru separarea funcțiilor													
	Grup de control	**Analist de sisteme**	**Programator de aplicații**	**Birou de informații și manager de informații**	**Utilizator final**	**Introducere de date**	**Operator PC**	**Administrator baze date**	**Administrator rețea**	**Administrator de sistem**	**Administrator securitate**	**Programator de sisteme**	**Asigurarea calității**
Grup de control		X	X	X		X	X	X	X	X		X	
Analist de sisteme	X			X	X		X				X		X
Programator de aplicații	X			X	X	X	X	X	X	X	X	X	X
Birou de informații și manager de informații	X	X	X		X	X		X	X	X		X	
Utilizator final		X	X	X			X	X	X			X	X
Introducere de date	X		X	X			X	X	X	X	X	X	
Operator PC	X	X	X		X	X		X	X	X	X	X	
Administrator baze de date													
Administrator rețea	X		X	X	X	X	X	X					
Administrator de sistem	X		X	X		X	X	X					
Administrator de securitate		X	X			X	X					X	
Programator de sisteme	X		X	X	X	X	X	X			X	X	X
Asigurarea calități		X	X		X								X
X – Alăturarea acestor funcții poate crea o potențială slăbire a securității													

Scopul segregării atribuţiilor este de a reduce sau elimina riscurile activităţii prin identificarea controalelor de compensare.

Controalele segregării atribuţiilor

Cerinţele de bună practică recomandă utilizarea unor anumite mecanisme de control pentru implementarea segregării atribuţiilor. În cele ce urmează vom prezenta pe scurt aceste mecanisme de control:

- *autorizarea tranzacţiilor* este responsabilitatea departamentului utilizatorilor. Autorizarea poate fi delegată unui persoane care prezintă un anumit nivel de responsabilitate. Managementul şi auditorul SI vor trebui să realizeze periodic teste pentru a verifica măsura în care se introduc în sistem date neautorizate;
- *custodia activelor* în cadrul organizaţiei trebuie determinată şi asignată adecvat. Proprietarul unor date este asignat de regulă unui departament şi atribuţiunile lui trebuie stabilite într-o formă scrisă. El are responsabilităţi legate de autorizarea nivelelor necesare pentru a asigura o securitate adecvată, în timp ce grupul de administrare este adesea responsabil pentru implementarea sistemului de securitate;
- *accesul la date*: controlul asupra accesului la date este dat de o combinare a unor elemente de securitate fizică, a sistemului şi aplicaţiei. Mediul fizic trebuie să fie securizat pentru a se preveni accesul unor persoane neautorizate la anumite echipamente conectate la unitatea centrală de procesare şi prin aceasta accesul la date. Elementele de securitate ale sistemului şi aplicaţiei reprezintă niveluri adiţionale de securitate care pot preveni obţinerea de către persoane neautorizate a accesului la date. O atenţie deosebită trebuie acordată accesului datelor de la distanţă.

Deciziile privind controlul accesului se bazează pe politica organizaţiei şi pe două standarde general acceptate: segregarea atribuţiilor şi ultimul privilegiu. Controlul accesului trebuie să acopere toate resursele organizaţiei, ceea ce implică o clasificare prealabilă a resurselor.

Politicile stabilesc nivelul de senzitivitate pentru date şi alte resurse: foarte secret, secret, confidenţial şi neclasificat. Această clasificare se recomandă a fi utilizată drept ghid în procedurile privind utilizarea resurselor informaţionale şi totodată pentru deciziile privind controlul accesului. Fiecare utilizator va trebui să fie autorizat să utilizeze numai acele resurse la un anumit nivel al senzitivităţii şi implicit la nivelurile inferioare acestuia.

Forme de autorizare

Managerii departamentelor trebuie să completeze pentru angajaţii din subordine formularele necesare autorizării utilizatorilor în sistem. Stabilirea autorizărilor se realizează în baza sarcinilor de serviciu, accesul fiind autorizat pentru anumite aplicaţii. În cazul organizaţiilor mari sau al organizaţiilor prezentând locaţii dispersate teritorial este necesară compararea semnăturilor din formularele de autorizare a accesului cu cele existente în jurnalele de semnături. Privilegiile acordate utilizatorilor privind drepturile de acces se vor revizui periodic pentru a se verifica măsura în care sunt adecvate în raport cu fişele posturilor.

Departamentul SI utilizează informaţiile înscrise în formele de autorizare pentru a completa şi actualiza tabele ale autorizărilor utilizatorilor. Aceste tabele vor reţine informaţia privind drepturile atribuite utilizatorilor privind consultarea, actualizarea şi/sau ştergerea datelor. Datorită informaţiei critice conţinute, aceste tabele trebuie securizate împotriva accesului neautorizat prin metode cum ar fi parolarea şi/sau criptarea. Pentru un control strict al accesului la aceste informaţii trebuie asigurată înregistrarea în jurnale automate a informaţiilor privind activităţile tuturor utilizatorilor, managementul cu responsabilităţi în domeniu având obligaţia să verifice periodic aceste jurnale. Este imperios necesară investigarea tuturor excepţiilor evidenţiate de respectivele jurnale.

Controale pentru compensarea nerespectării segregării atribuţiilor

Numărul limitat, uneori, de personal în departamentul IT determină alocarea de responsabilităţi prin respectarea parţială a principiului segregării atribuţiilor. În aceste

situaţii sunt necesare controale care să compenseze riscurile rezultate din alocarea responsabilităţilor. Controalele de compensare pot fi reprezentate de[6]:

- **auditul trail**: componentă ce se regăseşte în sistemele bine proiectate care permite reconstituirea traseului fiecărei tranzacţii. În absenţa segregării atribuţiilor, această facilitate poate constitui un bun control;
- **reconcilierea** este în ultimă instanţă responsabilitatea utilizatorilor. În unele organizaţii, grupul de control poate realiza reconcilieri parţiale ale aplicaţiilor prin utilizarea controlului la nivel de totaluri. Prin aceste verificări independente se asigură sporirea încrederii în funcţionarea corectă a aplicaţiilor;
- **raportarea** excepţiilor trebuie să reprezinte o modalitate de control la nivel persoanelor cu responsabilităţi de supervizare. Managementul trebuie să se asigure de faptul că excepţiile au fost corect soluţionate;
- **jurnalizarea tranzacţiilor** se poate realiza manual sau automat. Jurnalizarea manuală se poate realiza prin înscrierea tranzacţiilor (grupate pe loturi) înaintea trimiterii spre procesare. Jurnalizarea automată a tranzacţiilor se realizează de sistem pe măsura procesării acestora;
- **verificările supervizorilor** se pot realiza prin tehnica observării directe sau chestionării;
- **verificările independente** sunt realizate pentru corectarea erorilor sau compensarea eşecurilor intenţionate în desfăşurarea procedurilor stabilite. Aceste verificări pot conduce la identificarea erorilor şi deficienţelor.

2.10. Structura şi implementarea guvernanţei corporative

În procesul auditării funcţiei IT se recomandă a fi urmăriţi o serie de indicatori care pot atenţiona asupra unor probleme potenţiale:

- atitudini nefavorabile utilizatorilor finali;
- depăşiri ale bugetelor;
- depăşirea termenelor de finalizare a proiectelor;
- mişcări importante de personal;
- personal fără pregătirea şi experienţa necesare;

---

[6] Conform CISA.

- timp de răspuns neadecvat al sistemului;
- numărul important de proiecte abandonate sau suspendate;
- achiziții neautorizate de software și/sau hardware;
- frecvente upgrade-uri hardware și/sau software;
- numeroase rapoarte ale excepțiilor sau rapoarte ale excepțiilor nesoluționate;
- motivație redusă a personalului;
- bazarea pe una sau două persoane-cheie;
- lipsa unui training adecvat.

2.11. Revederea documentațiilor

Auditorul SI trebuie să procedeze la revizuirea următoarelor documente:

- *strategii, planuri și bugete TI*. Acestea oferă informații privind planificarea și controlul exercitat de management asupra mediului SI și măsura alinierii la strategia de business;
- *documentația politicii de securitate* deoarece aceasta oferă standardul pentru conformitate. Politica stabilește poziția organizației cu privire la riscurile de securitate, stabilind măsurile preventive necesare pentru protejarea activelor, inclusiv a datelor și programelor;
- *organigrame ale structurii organizatorice și diagrame funcționale*, acestea având rolul de a furniza informații necesare auditorului SI pentru înțelegerea subordonărilor și liniilor de raportare în cadrul departamentelor și organizației în ansamblul ei. În egală măsură, aceste documente pot oferi informații legate de segregarea atribuțiilor;
- *fișele posturilor* conțin informații extrem de importante cu privire la responsabilitățile și atribuțiile diferitelor poziții din cadrul organizației. Din analiza acestor documente se obțin informații privind segregarea atribuțiilor putându-se identifica posibile conflicte de interese. În baza fișelor posturilor se analizează nivelurile de raportare, conformitatea cu informația înscrisă în organigramă și nevoile derulării activității;
- *rapoartele comitetului de coordonare (steering committee)* oferă informații privind proiectele aflate în derulare. Conținutul acestor rapoarte este analizat

de managementul superior, iar informaţia este diseminată către departamentele implicate;

- *procedurile de modificare a sistemelor de dezvoltare şi programare* oferă informaţii privind cadrul realizării acestor schimbări;
- *proceduri de operare* oferă informaţii privind responsabilităţile personalului cu atribuţii de operare;
- *manualele departamentului de personal* sunt importante prin informaţia oferită privind regulile şi reglementările interne legate de conduita angajaţilor;
- *procedurile de asigurare a calităţii* oferă cadrul şi standardele ce trebuie urmate de departamentul SI.

Auditorul SI va proceda la analiza contractelor încheiate pentru procurarea hardware-ului, software-ului şi serviciilor SI, urmărind: clauzele, procesul de selecţie a partenerilor, modul de derulare a contractelor, probleme de conformitate. Toate aceste aspecte vor fi analizate prin prisma autorizărilor date de management, a documentelor legale existente, a implicării managementului în procesul contractării.

2.12. Test de evaluare a cunoştinţelor

1. Comitetul de coordonare *(steering committee)* al SI trebuie:
   a. să includă membrii din diferite departamente şi cu niveluri de pregătire profesională diferite;
   b. să se asigure că politicile şi procedurile de securitate ale SI au fost executate corespunzător;
   c. să aibă un plan de discuţii şi să acorde timp pentru acest plan, în întâlnirile de lucru;
   d. să cunoască noile tendinţe şi produse din domeniul TI la fiecare întâlnire cu furnizorii.
2. Guvernanţa TI este responsabilitatea primară a:
   a. ofiţerului şef de execuţie;
   b. comitetului director;
   c. comitetului de coordonare TI;

d. comitetului de audit.

3. Guvernanța TI efectivă asigură de fapt că planul TI este în conformitate cu:

a. planul de afaceri;
b. planul de audit;
c. planul de securitate;
d. planul de investiții.

4. Un administrator de rețea locală (LAN), în mod normal, ar trebui să nu aibă responsabilități privind:

a. utilizatorii finali;
b. raportarea către conducerea utilizatorilor finali;
c. activitatea de programare;
d. administrarea securității la nivel LAN.

5. Care dintre următoarele elemente sunt considerate de un auditor ca fiind cele mai relevante pentru planificare pe termen scurt, într-un departament SI?

a. alocarea resurselor;
b. aducerea la cunoştinţă a tehnologiilor avansate;
c. conducerea unui control de autoevaluare;
d. evaluarea necesarului de componente hardware.

6. Un auditor SI care analizează planul strategic al unei societăți ar trebui să analizeze în primul rând :

a. mediul TI existent;
b. planul de afaceri;
c. bugetul alocat TI în prezent;
d. tendințele actuale ale tehnologiei.

7. Riscurile asociate de culegerea evidențelor electronice, ar trebui să fie cel mai probabil reduse printr-un e-mail, prin :

a. politici de distrugere;
b. politici de securitate;
c. politici de arhivare;
d. politici de auditare.

8. Lipsa controalelor de securitate adecvate reprezintă:

a. o ameninţare;
b. un bun (o resursă informaţională);
c. un impact;
d. o vulnerabilitate.

9. Care dintre următoarele afirmaţii este un mecanism pentru minimizarea riscurilor:

a. practici de control şi securitate;
b. asigurarea responsabilităţilor şi proprietăţii;
c. auditul şi certificarea;
d. contractele şi acordurile la nivel de service (SLA).

10. Când dezvoltăm un program de management al riscului, prima activitate ar trebui să fie:

a. evaluarea ameninţărilor;
b. clasificarea datelor:
c. inventarierea bunurilor;
d. analiza activităţilor critice.

Capitolul 3
Managementul ciclului de viață al sistemului informațional

Capitolul 3

Managementul ciclului de viață al sistemului informațional

3.1. Ciclul de viață al sistemului informațional

Un *sistem informațional* (*Information System* - IS) este un ansamblu de procese, proceduri și echipamente folosite pentru culegerea, transmiterea, stocarea și procesarea datelor în vederea obținerii informațiilor necesare în procesul decizional al organizației. În literatura anglo-americană, deși se face distincție între „*information system*" (sistem informațional) și „*computer based information system*" (ceea ce la noi s-a încetățenit ca fiind „sistem informatic"), datorită nivelului tehnologic și gradului ridicat de automatizare a activităților informaționale la care s-a ajuns, specialiștii, după ce fac delimitarea amintită, folosesc termenul de „*information system*".

Ciclul de dezvoltare al sistemelor informaționale reprezintă pașii de urmat pentru realizarea unui sistem informațional dedicat rezolvării unei anumite probleme informaționale, adică a unei probleme legate de culegerea, stocarea, transformarea și furnizarea datelor în conținutul, structura și forma cerute de utilizatori. Structura ciclului de dezvoltare a unui SI este determinată de logica activităților necesare pentru obținerea sa.

Sistemul informațional, ca orice entitate a lumii reale, prezintă propriul său *ciclu de viață*. Punctul de început al acestui ciclu este reprezentat de decizia de realizare a unui nou SI, iar punctul final este reprezentat de înlocuirea SI existent cu un SI nou, mai bine adaptat cerințelor, asigurând performanțe informaționale, tehnice și economice superioare.
În cadrul ciclului de viață se disting două etape: dezvoltarea SI și exploatarea.

Orice proiect al SI de tehnologia informației (TI), care presupune dezvoltarea unui SI sau o infrastructură nouă, începe cu un studiu al sistemului informațional existent, cunoscut adesea ca *studiu de fezabilitate* care identifică domeniul (aria) problemei, analizează SI existent, identificând punctele slabe și forte ale acestuia, stabilește cerințele noului sistem, explorează soluții posibile și face recomandări privind calea care trebuie urmată.

După finalizarea studiului de fezabilitate se elaborează *studiul de caz al afacerii* care trebuie să fie suficient de detaliat pentru a descrie justificările de demarare şi de continuare a proiectului.

Dacă în orice etapă, studiul de caz al afacerii evidenţiază deteriorarea performanţei prin creşterea costurilor sau o reducere anticipată a beneficiilor, finanţatorul proiectului sau comitetul de conducere trebuie să decidă dacă proiectul va continua sau nu. Dacă studiul de caz al afacerii se schimbă pe parcursul dezvoltării unui proiect de TI, proiectul va trebui reaprobat.

În cazul unui proiect de dezvoltare a unui SI, beneficiile nu se obţin imediat, ci pe parcursul ciclului de viaţă al acestuia. Împreună cu studiul de caz al afacerii, la începutul unui proiect de dezvoltare a SI trebuie făcută o planificare a realizării beneficiilor, ce trebuie apoi urmărită printr-un proces de management al acestora, care cuprinde:

- validarea beneficiilor previzionate în afacere;
- planificarea beneficiilor care trebuie realizate;
- măsurarea beneficiilor în raport cu obiectivele stabilite;
- stabilirea responsabilităţilor-cheie pentru realizarea beneficiilor.

Datorită complexităţii activităţii dezvoltării şi întreţinerii sistemelor informaţionale, cât şi datorită riscurilor pe care le implică, alături de *latura* numită *tehnică*, ce cuprinde activităţile necesare conceperii şi realizării procedurilor, sunt necesare şi o serie de *activităţi-suport*. Una dintre acestea vizează *managementul proiectelor* şi include subactivităţi de planificare, organizare, execuţie şi monitorizare.

O altă activitate-suport vizează *managementul schimbărilor şi al configuraţiei*, unde sunt cuprinse aspectele legate de *dezvoltarea paralelă*, dezvoltarea pe site-uri diferite, gestionarea versiunilor intermediare ale produsului, raportarea şi remedierea erorilor etc. În sfârşit, o altă activitate-suport se referă la *asigurarea mediului de dezvoltare* şi vizează adaptarea procesului de bază şi a instrumentelor software la specificul SI aflat în curs de realizare.

3.2. Managementul proiectelor privind dezvoltarea şi întreţinerea sistemelor informaţionale

3.2.1. Aspecte comune privind organizarea şi conducerea proiectelor de tehnologia informaţiei (TI)

Din punct de vedere istoric, conceptul de management de proiect a apărut în anii '60, odată cu dezvoltarea programelor spaţiale în SUA. Apariţia unor instrumente grafice de planificare cum sunt graficul GANTT[1] sau graficul PERT[2] şi aplicarea practică a

---

[1] Graficul GANTT – inventat de Henry L. Gantt.

[2] Graficul PERT – (acronim din limba engleză – *Program Evaluation Review Tehnique* - Tehnica Verificării Evaluării Programului).

managementului prin obiective la conducerea programelor şi proiectelor au avut o importanţă deosebită la lărgirea sferei de aplicare a acestui concept în practică şi transformarea sa într-o disciplină ştiinţifică managerială, de sine stătătoare.

Un proiect este o succesiune de etape şi activităţi care, planificate într-o perioadă limitată de timp şi cu resursele aferente, conduc la realizarea unui obiectiv ce derivă dintr-o strategie stabilită anterior. Programele pot fi considerate sisteme complexe prin care resursele financiare, umane şi materiale, stabilite prin politici şi consolidate prin strategii, se materializează prin intermediul proiectelor în efecte benefice.

Un program poate fi văzut ca un grup de proiecte şi sarcini limitate în timp care sunt strâns legate între ele prin obiective comune, buget comun, planificare şi strategii. Întocmai ca şi proiectele, programele trebuie să se încadreze într-un interval de timp (data de început şi data de sfârşit) şi în limitele organizaţiei.

Un exemplu tipic de program este dezvoltarea sistemelor informaţionale integrate de întreprindere (*Entreprise Resources Planing* - ERP), cum ar fi de exemplu SAP incluzând: infrastructura, tehnologia, operaţii, procese de reengineering (*Business Process Reengineering* - BPR) şi optimizare, training şi dezvoltare, adaptare la cerinţele organizaţiei.

Pentru a face posibilă autonomia proiectelor, pe de o parte, şi a utiliza sinergia dintre proiecte, pe de altă parte, este necesară o organizare a programului în care actorii principali sunt: proprietarul, managerul echipei de realizare a programului şi personalul auxiliar. Structura tipică de comunicare într-un program constă în întâlnirile de lucru ale proprietarului programului şi întâlnirile de lucru ale echipei de realizare a programului.

Portofoliul de proiecte este definit ca ansamblul proiectelor existente şi în curs de realizare într-o organizaţie la un moment dat. În contrast cu managementul unui program, în care toate proiectele relevante sunt cuplate între ele, aceasta nu este o cerinţă şi într-un portofoliu de proiect. Trebuie avut însă în vedere faptul că proiectele unui program aparţin bineînţeles portofoliului de proiecte al companiei.

Obiectivele managementului portofoliului de proiecte sunt:
- optimizarea rezultatelor la nivelul portofoliului de proiecte (nu proiectelor individuale);
- prioritizarea şi programarea proiectelor;
- coordonarea resurselor (interne şi externe);
- cunoaşterea transferului între proiectele din portofoliu.

Metodologia şi procesele utilizate în managementul programului sunt foarte asemănătoare cu cele ale managementului proiectelor, care se pot derula în paralel unele cu altele. Pentru a începe în mod oficial un program, sunt absolut necesare

unele forme de angajament scris ale finanțatorului către managerul de program și echipa de realizare a programului.

Pentru a se angaja în managementul unui program, al unui portofoliu de proiecte și în managementul proiectelor, o organizație are nevoie de structuri specifice și bine definite, cum ar fi o echipă de experți, un birou de management al proiectelor și un grup de portofoliu de proiecte. Acestea folosesc instrumente integrative specifice, cum ar fi: ghiduri de management al proiectelor, planuri de proiecte standard și instrumente de marketing al managementului proiectelor. Biroul de management al proiectului trebuie să fie o structură permanentă și adecvată, cu personal care să mențină suportul profesional în această zonă, să întrețină procedurile curente și să dezvolte noi proceduri și standarde. Acest obiectiv are în vedere îmbunătățirea proiectului și a calității managementului de program, precum și asigurarea succesului proiectului. Dar, în aceeași măsură, trebuie să se concentreze numai pe activități și sarcini care provin din această zonă (procesul de management al proiectului) și nu asupra conținutului proiectului sau al programului. Astfel, un auditor trebuie să decidă între auditarea conținutului proiectului și/sau aspectele procedurale ale programelor sau proiectelor.

Orice proiect are un obiectiv specific care trebuie realizat cu îndeplinirea unor cerințe privind data de început și data de sfârșit, limitări financiare și consumul de resurse în termeni de bani, echipamente și materiale. Datorită acestor caracteristici, un proiect poate fi cel mai bine reprezentat printr-un triunghi ale cărui laturi reprezintă *durata, costurile și rezultatele previzionate*.

Managementul de proiect presupune realizarea unui echilibru între restricțiile de timp, cost și rezultate. Triunghiul care reprezintă proiectul ilustrează procesul de realizare a echilibrului între restricții, întrucât cele trei laturi ale triunghiului sunt interdependente, iar schimbarea mărimii unei laturi a triunghiului afectează cel puțin una dintre celelalte două laturi.

Astfel:

- dacă *durata* proiectului scade, ar putea fi necesară suplimentarea *bugetului*, fiind necesare resurse suplimentare. În măsura în care *bugetul* nu poate fi suplimentat, se poate lua decizia de a modifica obiectivele, nemaiputând fi realizate toate activitățile planificate. Există riscul ca, prin micșorarea *duratei* de realizare a proiectului, să se modifice calitatea globală a proiectului. De exemplu, testarea și controlul calității au loc, de obicei, la sfârșitul unui proiect de dezvoltare SI; dacă durata proiectului este micșorată ulterior, este posibil să se renunțe chiar la aceste ultime activități, cu efect direct asupra calității SI;
- reducerea *bugetului* necesită de cele mai multe ori analiza posibilității înlocuirii anumitor categorii de resurse cu altele mai ieftine, dintr-o clasă inferioară, care corespund totuși utilizării dorite (de exemplu un calculator cu o capacitate mai

mică sau cu o viteză mai slabă, sau un calculator cu o configurație minimală pentru stadiul inițial al proiectului etc.). În mod similar, putem înlocui un personal specializat, care solicită un salariu mai mare, cu altul cu mai puțină experiență și salariu mai mic pentru executarea unor activități mai puțin pretențioase. De obicei, reducerea bugetului poate determina realizarea unor SI cu performanțe reduse față de cele stabilite inițial;
- schimbarea obiectivului unui proiect pe parcursul realizării acestuia se numește obiectiv extins și necesită de cele mai multe ori refacerea bugetului și replanificarea activităților.

Obiectivele proiectului trebuie să fie realizate:
- la timp (în durata prevăzută);
- în bugetul prevăzut;
- cu nivelul de performanță și specificațiile cerute;
- cu utilizarea eficientă și eficace a resurselor;
- cu acordul clientului.

Un proiect trebuie să aibă în mod clar definite obiectivele specifice, care să fie măsurabile, realizabile, relevante și limitate în timp. Aceste obiective pot fi clasificate în obiective principale, adiționale și nonobiective.

Obiectivele principale trebuie să fie asociate întotdeauna cu succesul afacerii. *Obiectivele adiționale* sunt obiectivele care nu au în mod direct legătură cu rezultatele proiectului, dar pot contribui la succesul acestuia (reorganizarea afacerii într-un proiect de realizare a software-ului). *Nonobiectivele* adaugă claritate scopului și fac mai vizibile limitele proiectului, conturează mai bine părțile care vor fi livrate și vor susține toate părțile pentru a câștiga o bună înțelegere asupra a ceea ce trebuie făcut și a înlătura orice ambiguități.

3.2.2. Structuri în managementul proiectelor

Una dintre deciziile pe care managerul de proiect trebuie să o ia și pe care apoi să o transmită organizației de care aparține este tipul de structură organizațională care să fie cea mai adecvată pentru realizarea proiectului. În majoritatea cazurilor, managerul de proiect va dori să aibă o „echipă pentru proiect" care să lucreze pentru el, constituită din membrii biroului de proiectare și din toți specialiștii operaționali de care are nevoie doar pentru proiectul său, și nu pentru altceva. Această situație este rar întâlnită, întrucât sunt alte proiecte în curs de execuție care, de asemenea, au nevoie de specialiști. De asemenea, managerii nu sunt dispuși să îi detașeze pe cei mai capabili angajați pe perioade mari de timp. Astfel, limitarea resurselor a condus la structura organizațională de tip „matrice", în care specialiștii sunt împărțiți între diferite proiecte și divizii funcționale.
Contextul proiectului poate fi divizat într-un context social și de timp. În analiza conținutului contextului trebuie ținut cont de:

- importanța proiectului în organizație;
- conexiunea dintre strategia organizației și proiect:
- relațiile dintre proiect și celelalte proiecte;
- conexiunea dintre fazele proiectului.

Câtă vreme, în mod normal, se desfășoară mai multe proiecte în același timp, relațiile dintre aceste proiecte trebuie să fie investigate pentru a identifica obiectivele comune ale afacerii organizației, pentru a identifica și gestiona riscurile, dar și pentru a identifica conexiunile dintre resurse. O abordare comună în acest sens presupune stabilirea unui management de portofoliu de proiecte și/sau o structură de management de program.

Un manager de proiect TI trebuie să fie identificat și numit de comitetul de coordonare al proiectului. Managerului de proiect, care nu trebuie să fie un membru SI, pentru succesul complet al proiectului, trebuie să i se acorde controlul operațional complet asupra proiectului și să-i fie alocate resursele necesare, incluzând profesioniști și membri ai altor departamente. *Auditorii SI trebuie să fie incluși în echipa proiectului ca experți de control.* Rolul lor este de a furniza un punct de vedere independent și obiectiv pentru a asigura că nivelul de implicare (angajare) a părților responsabile este corespunzător. În aceste situații, auditorii SI nu execută un audit, dar participă în proiect cu rol de consultanți.

Comunicarea și cultura proiectului

Depinzând de mărimea și complexitatea proiectului și a părților implicate, la inițierea procesului de management al proiectului comunicarea trebuie să fie realizată prin:
- întâlniri de lucru;
- întâlniri de lucru neprotocolare;
- întâlniri de lucru privind demararea proiectului;
- o combinație a acestora.

Ca sistem social independent, fiecare proiect are cultura proprie, care îi definește normele și regulile de angajament. Cultura proiectului nu poate fi descrisă, dar se manifestă ea însăși în modul de aplicare a tehnicilor de management ale proiectului, incluzând planificarea proiectului, formele de comunicare etc.

Metodele de dezvoltare a culturii proiectelor includ stabilirea misiunii proiectului, a unui nume și logoul proiectului, regulile întâlnirilor echipei proiectului, protocoalele de comunicare și evenimentele de popularizare a acestora.

Responsabilităţi privind managementul proiectelor SI

Pentru a asigura succesul complet şi implementarea oricărui sistem nou, trebuie ca auditorul să aibă o participare activă pe parcursul ciclului de viaţă al dezvoltării SI, acesta trebuind să se asigure că noul SI va beneficia de cele mai adecvate controale, începând din faza de proiectare şi terminând cu implementarea sistemului.

Dezvoltarea unui SI presupune următoarele roluri şi responsabilităţi (figura 3.1.1):

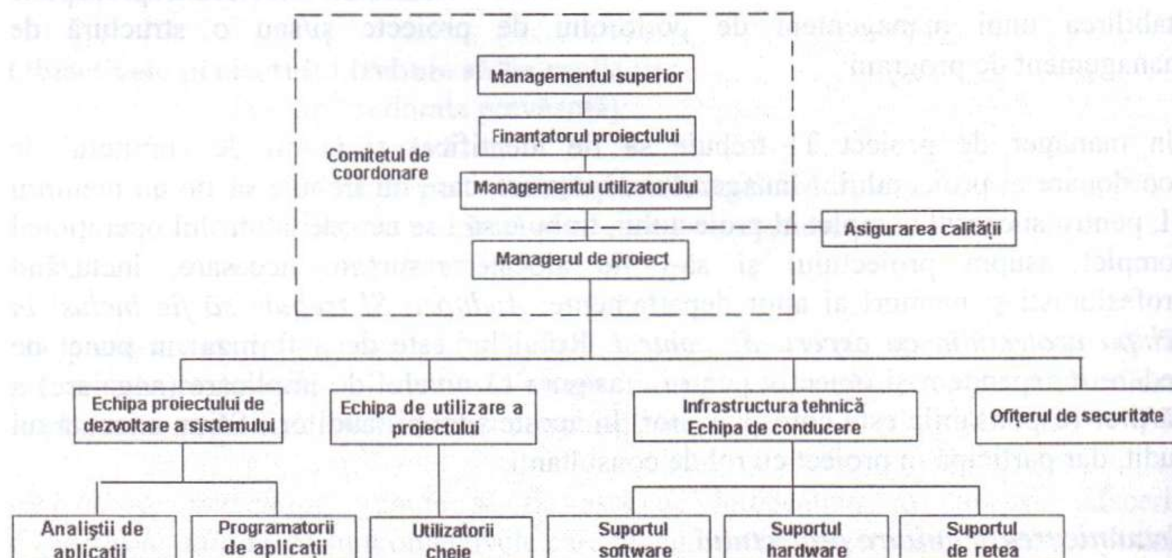


Figura 3.1.1. **Entităţile dezvoltării SI**

Managementul superior (*Senior Management*) susţine angajamentul pentru proiect şi aprobă resursele necesare realizării acestuia.

Managementul utilizatorului (*User Management*) îşi asumă rolul de proprietar al proiectului şi al rezultatului acestuia, participă activ în reproiectarea proceselor de afaceri, de definire a cerinţelor sistemului, defineşte teste de validare a sistemului pe parcursul dezvoltării acestuia, precum şi în faza finală de acceptare. În plus, se ocupă de pregătirea utilizatorilor în vederea preluării SI pentru exploatare.

Acesta trebuie să evalueze dacă SI în forma finală corespunde cu cerinţele formulate iniţial, răspunzând la următoarele întrebări: sunt funcţiile solicitate disponibile în SI?; cât de adaptabil este SI?; cât de eficient este SI?; este SI uşor de utilizat?; cât de uşor se pot transfera sau adapta date din vechiul SI în noul SI?; cât de uşor este de a transfera softul într-un nou mediu?; sunt posibile adăugări de noi funcţii? (sistemul este flexibil?).

Comitetul de coordonare a proiectului (*Projects Steering Committee*) reprezintă interesele principalilor acționari și este în ultimă instanță responsabil pentru atingerea obiectivului, costul proiectului și timpul de realizare. Acest comitet trebuie să includă un manager superior din fiecare sferă a afacerii, care va avea impact semnificativ în a propune un nou sistem sau în a propune modificarea sistemului. Fiecare membru trebuie să aibă autoritatea de a lua decizii în proiectarea sistemului, decizii care ar afecta departamentul în care aceștia își desfășoară activitatea. Conducerea acestui proiect este asigurată în majoritatea cazurilor de finanțatorul proiectului. Managerul proiectului trebuie să fie de asemenea membru în acest comitet și în unele cazuri poate să asigure rolul de șef al comitetului. Funcțiile acestui comitet sunt: de a revedea cu regularitate evoluția proiectului (o dată sau de două ori pe lună); de a convoca întâlniri de urgență când este cazul; de a servi drept coordonator și consilier. Membrii comitetului trebuie să fie disponibili în a răspunde întrebărilor și a da informații cu privire la sistem și la desfășurarea programului, fiind în măsură să ia măsuri corective, dacă acestea sunt necesare. Comitetul trebuie să evalueze stadiul proiectului și să acționeze sau să vină cu recomandări privind schimbări de personal în cadrul echipei proiectului, să facă modificări în bugete și programarea lor, să aducă schimbări în obiectivele proiectului și să intervină în cadrul redefinirii proiectului. Comitetul trebuie să identifice riscurile și să evidențieze sarcinile care sunt în dificultate și care nu pot fi rezolvate la nivelul proiectului. Managerul de proiect trebuie să aibă abilitatea să escaladeze dificultățile respective și, în beneficiul organizației, să se bazeze pe acest comitet în soluționarea problemelor. În anumite situații, comitetul poate recomanda inclusiv oprirea proiectului.

Finanțatorul proiectului (*Project Sponsor*) furnizează fonduri și cuantifică proiectul; lucrează în consens cu managerul de proiect pentru a defini factorii critici de succes ai proiectului. Acesta este și proprietarul datelor și al aplicației. Finanțatorul proiectului este manager superior la conducerea primei unități care va utiliza sistemul.

Managementul dezvoltării infrastructurii (*Systems Development Management*) furnizează suportul tehnic privind infrastructura hardware și software pentru dezvoltarea, instalarea și operarea SI proiectat. Totodată, acesta trebuie să asigure compatibilitatea SI cu infrastructura existentă, direcțiile strategice ale TI, precum și suportul de operare și întreținere a SI după instalare.

Managerul de proiect (*Project Manager*) asigură conducerea zilnică a proiectului și urmărește ca acesta să se încadreze în direcțiile propuse inițial.

Principalele atribuții ale managerului de proiect: asigură aderarea proiectului la standardele locale, asigură că rezultatele parțiale și finale corespund din punct de vedere cantitativ și calitativ cu așteptările acționarilor, rezolvă conflictele interdepartamentale, monitorizează și controlează costurile și calendarul proiectului. Această persoană poate să fie un utilizator final, un membru al echipei de dezvoltare a

sistemului sau un manager de proiect profesionist. Acolo unde proiectele sunt realizate de personal dedicat, managerul de proiect stabileşte principalele responsabilităţi pentru acest personal.

Echipa de dezvoltare a sistemului (*Systems Development Project Team*) execută sarcinile atribuite, comunică în mod efectiv cu utilizatorii prin implicarea activă a acestora în procesul de dezvoltare, lucrează respectând standardele locale şi semnalează managerului de proiect situaţii în care apar abateri de la plan.

Echipa utilizatorului (*User Project Team*) execută sarcinile atribuite, comunică în mod efectiv cu echipa de dezvoltare a sistemului prin implicarea personală în procesul de dezvoltare, lucrează în concordanţă cu standardele locale şi semnalează managerului de proiect situaţiile de neconcordanţă faţă de planul stabilit.

Ofiţerul de securitate (*Security Officer*) asigură implementarea unui sistem de controale şi procese pentru protecţia efectivă a datelor pe baza clasificării acestora în concordanţă cu politicile şi procedurile de securitate ale organizaţiei. Analizează pe tot parcursul ciclului de viaţă măsurile de securitate care trebuie încorporate în sistem; revizuieşte planul testelor de securitate şi rapoartele pe care le primeşte la implementare; evaluează documentele de securitate pentru acreditarea sistemului. În mod periodic, monitorizează securitatea efectivă a sistemului în timpul ciclului de viaţă al acestuia.

Asigurarea calităţii (*Quality Assurance*) analizează rezultatele parţiale şi finale şi verifică măsura în care acestea corespund cerinţelor iniţiale.

Obiectivele specifice ale funcţiei de asigurare a calităţii includ:

- asigurarea participării active şi coordonate a tuturor părţilor implicate în revizia, evaluarea şi diseminarea standardelor, stabilirea liniilor directoare şi a procedurilor de management;
- respectarea metodologiei de dezvoltare a sistemului;
- revizuirea şi evaluarea proiectului în fazele semnificative de dezvoltare, venind cu recomandări în scopul îmbunătăţirii acestuia;
- stabilirea, punerea în evidenţă şi menţinerea unui mediu stabil şi controlat pentru implementarea schimbărilor din mediul de producere a SI;
- definirea, stabilirea şi menţinerea unui standard corespunzător privind metodologia de testare a SI;
- informarea managementului despre sistemele care nu funcţionează aşa cum au fost definite sau proiectate.

Este esenţial pentru auditorul SI să înţeleagă metodologia de dezvoltare, achiziţie şi întreţinere a SI utilizată şi să identifice potenţialele vulnerabilităţi şi punctele de control ale acestora. În cazul în care controalele lipsesc (ca rezultat al structurii

organizației sau al metodelor utilizate) sau procesul este dezordonat, rolul auditorului SI este de a sfătui managerul și echipa proiectului privind deficiențele cu care se confruntă.

3.2.3. Planificarea, realizarea și controlul proiectelor SI

Managementul proiectelor SI este bazat pe analiza resurselor și presupune aplicarea unor cunoștințe, aptitudini, instrumente și tehnici specifice pe tot parcursul etapelor de inițiere, planificare, executare, control și finalizare a acestora. Spre exemplu, programele *Microsoft Project Manager* sau *Primavera* sunt utilizate cu succes pentru planificarea, alocarea și urmărirea utilizării resurselor în cadrul proiectelor de SI.

Un proiect este inițiat de managerul de proiect care trebuie să dețină toate informațiile cerute pentru a obține aprobările în vederea realizării proiectului.

Una dintre etapele critice ale oricărui proiect este etapa de planificare, care determină ceea ce trebuie realizat, de cine, precum și termenele limită, pentru ca proiectul să se finalizeze la termenul stabilit. Rezultatele planificării vizează: eliminarea sau reducerea incertitudinii; îmbunătățirea eficienței în exploatare; mai buna înțelegere a obiectivelor; asigurarea unei baze pentru activitatea de monitorizare și control.

În această etapă, managerul de proiect trebuie să determine:
- sarcinile care trebuie îndeplinite pentru realizarea aplicațiilor SI;
- ordinea de executare a sarcinilor;
- durata sau timpul alocat pentru fiecare sarcină în parte;
- prioritatea fiecărei sarcini;
- resursele TI disponibile și necesare pentru a executa aceste sarcini;
- bugetul sau costul pentru fiecare dintre aceste sarcini;
- sursa fondurilor.

În continuare, vor fi prezentate câteva tehnici mai importante utilizate pentru planificarea și urmărirea proiectelor de SI.

Planificarea este orientată în principal spre dezvoltarea obiectivelor care sunt realiste și cuantificabile. Aceste obiective includ calitatea, performanța, întreținerea, fiabilitatea, operabilitatea, garanția produsului și conformitatea cu standardul stabilit.

Estimarea dimensiunii SI poate fi utilizată pentru a direcționa alocarea resurselor, estimarea timpului și a costului cerut pentru dezvoltarea sa, cât și pentru o comparare a efortului total necesar și al resurselor disponibile.

Metoda cea mai simplă și mai utilizată pentru determinarea dimensiunii SI constă în determinarea numărului de linii de cod sursă (SLOC); kilolinii de cod (KLOC) sau în

mii de instrucţiuni livrate (KDSI). Această metodă este aplicabilă când se utilizează limbaje de programare structurată cum ar fi BASIC sau COBOL. Tehnologii recente au introdus elemente de dezvoltare care adaugă una sau mai multe dimensiuni de estimare a dimensiunii SI.

Acestea iau acum formele unor reprezentări mai abstracte, cum ar fi diagrame, obiecte, celule de calcul, interogări de baze de date şi interfaţa grafică cu utilizatorul (*graphical user interface* - GUI).

O altă metodă, **analiza punctelor funcţionale** (*function point analysis* - FPA) a fost dezvoltată după 1970 şi a fost larg utilizată pentru a exprima complexitatea în dezvoltarea SI de mari dimensiuni. Rezultatul FPA este o măsură a dimensiunii unui sistem informaţional bazat pe puncte care se acordă în funcţie de complexitatea intrărilor, ieşirilor, fişierelor, interfeţelor şi interogărilor. Aceasta este o măsură indirectă a dimensiunii software şi a procesului prin care este dezvoltat versus măsura orientată direct, cum ar fi SLOC. Punctele funcţionale (FPs) sunt calculate printr-o tabelă (tabelul 3.2.1).

Tabelul 3.2.1. **Punctele funcţionale**

Calculul punctelor funcţionale					
Parametrul de măsură	**Calcul**	**Factorul de greutate**			
		Simplu	**Mediu**	**Complex**	**Rezultate**
Numărul de intrări ale utilizatorului		3	4	6	–
Numărul de ieşiri ale utilizatorului		4	5	7	–
Numărul de cerinţe ale utilizatorului		3	4	6	–
Numărul de fişiere		7	10	15	–
Numărul de interfeţe externe		5	7	10	–
Total:					
Notă: Utilizarea metodei FP necesită stabilirea unor criterii pentru a determina dacă o intrare particulară este simplă, medie sau complexă					

După completarea intrărilor tabelei, determinarea punctelor funcţionale se face printr-un algoritm care ia în considerare şi: credibilitatea, complexitatea, reutilizarea, schimbarea, portabilitatea şi punctele critice. Punctele funcţionale sunt apoi utilizate într-o manieră analogă estimării SLOC, ca o măsură pentru cost, planificare, productivitate şi calitate măsurabilă (productivitate = FP/persoană pe lună, calitate = defecte/FP, cost = $/FP).

În cele mai multe aplicații standard, funcțiile sistemului sunt identificate și efortul corespondent este estimat. În dezvoltarea aplicațiilor WEB, efortul depinde de numărul de ecrane (forme), numărul de imagini, tipul imaginilor (statice sau animate), interfețe și referințe încrucișate care sunt solicitate. Astfel, din punctul de vedere al aplicațiilor WEB, efortul de realizare va include, pe lângă punctele funcționale, și trăsăturile specifice ale acestora.

Pentru stabilirea bugetului necesar proiectului de SI trebuie estimate eforturile privind:
- numărul de ore alocat fiecărui membru al echipei;
- orele de utilizare a echipamentelor (predomină timpul de utilizare a calculatorului în aceeași măsură cu facilitățile de duplicare, echipamente de birou și echipamente de comunicare);
- alte costuri externe, cum ar fi alte tipuri de softwareul, licențele instrumentelor pentru proiect, costul contractelor de consultanță, costurile de întreținere, costurile de certificare (dacă este cazul) și costurile de întreținere sau chirie (dacă pentru proiect este necesar un spațiu suplimentar).

Având estimarea eforturilor umane pentru fiecare activitate, prin însumarea acestora se obțin eforturile pe faze de proiect care, mai departe, multiplicate cu tarifele orare, permit determinarea bugetului proiectului.

Bugetul reflectă eforturile financiare privind resursele umane și utilizarea elementelor implicate în realizarea proiectului. Planificarea implică stabilirea ordinii de execuție a activităților proiectului și necesită informații privind datele de început și de sfârșit stabilite a acestora.

Planificarea poate fi reprezentată în mod grafic utilizând tehnici variate, cum ar fi diagrame PERT sau grafice GANTT. În anumite puncte-cheie din cadrul proiectului, bugetul și planificarea trebuie revăzute pentru a verifica conformitatea și pentru a identifica neconcordanțele și a interveni cu acțiuni corective. Graficul GANTT este un instrument de reprezentare a unui proiect în funcție de timp sau de cost. O activitate reprezintă totalul lucrărilor care trebuie efectuate într-un anumit interval de timp. Graficul arată când trebuie să înceapă o activitate și când trebuie să ia sfârșit. Evenimentele sunt descrise fie ca punct de pornire, fie ca punct final pentru una sau mai multe activități. Graficul poate, de asemenea, reflecta resursele atribuite fiecărei activități și procentul de alocare a acestora. Diagramele GANTT nu prezintă legăturile dintre activități, ci numai perioadele de începere și încheiere.

PERT este o tehnică de management al proiectelor reprezentate sub forma unei rețele, utilizată adesea în dezvoltarea sistemelor bazate pe evenimente și activități. Fiecare activitate este caracterizată de trei timpi:

- a = cel mai optimist timp de finalizare; acest timp presupune că totul va merge conform planului, cu minimum de dificultăţi;
- b = cel mai pesimist timp de finalizare; acest timp presupune că nimic nu merge conform planului şi există un număr maxim de dificultăţi care pot interveni;
- m = cel mai probabil timp de finalizare; acesta este timpul care după opiniile managerilor operativi este considerat a fi realizabil.

Timpul optim calculat (tc) va fi: tc=(a+4m+b)/6.

Pentru a reprezenta un proiect de SI printr-o reţea PERT, trebuie să cunoaştem pentru fiecare activitate care sunt activităţile precedente, activităţile succesoare şi ce activităţi pot fi desfăşurate în paralel. Pe baza reţelei PERT se poate aplica un algoritm care determină drumul critic (*Critical Path Method*), care este cel mai lung drum din reţea, ale cărui activităţi au rezerva de timp = 0.

Timebox Management este o altă tehnică utilizată pentru managementul proiectelor de SI într-o perioadă relativ scurtă şi fixă de timp, cu resurse specifice predeterminate, punându-se în balanţă calitatea software-ului şi cerinţele de livrare stabilite iniţial.

Această tehnică corespunde foarte bine managementului proiectelor de SI care se bazează în principal pe obiective punctuale, formulate de utilizatorii finali şi utilizează metode de realizare care să permită finalizarea proiectului într-o perioadă limitată de timp.

Avantajul major al acestei abordări constă în faptul că previne creşterea peste măsură a costurilor şi întârzieri de la livrările planificate. Fazele de proiectare şi realizare a SI sunt scurtate datorită utilizării tehnicilor şi instrumentelor noi, cum sunt prototipul şi dezvoltarea rapidă de aplicaţii. Cerinţele de testare, pregătirea testului şi acceptarea acestuia sunt uşor de stabilit prin participarea directă în echipa de proiect a utilizatorilor finali.

O componentă importantă a managementului unui proiect de SI este controlul asupra obiectivelor, alocării resurselor necesare realizării acestora şi riscurilor aferente nerealizării obiectivelor. Toate schimbările care apar pe parcursul derulării proiectului trebuie bine argumentate, documentate şi aprobate, astfel încât să corespundă eforturilor investitorilor.

Finalizarea (închiderea) proiectului este momentul în care SI trece din producţie în exploatare de către utilizatorii finali. Cu acest prilej, finanţatorul proiectului constată dacă SI corespunde cerinţelor formulate iniţial şi stabileşte proprietarii SI care vor prelua programele, documentaţiile de exploatare a acestora şi se vor ocupa mai departe de implementare. Totodată se face o analiză a modului de realizare a proiectului, scoţându-se în evidenţă punctele tari şi slabe, pentru a servi ca lecţii şi bune practici pentru proiecte viitoare.

3.3. Metode de dezvoltare a SI

3.3.1. Metoda SDLC (*Systems Development Life Cycle*)

Abordarea dezvoltării tradiționale a ciclului de viață al sistemului[3]

Dezvoltarea unui SI nou este generată de una dintre următoarele situații:
- o oportunitate nouă relativă la un proces de afacere nou sau existent;
- o cerință informațională nouă relativă la un proces de afacere existent;
- o oportunitate nouă care permite organizației să obțină avantaje tehnologice;
- introducerea unei tehnologii noi, mai performante decât cele existente.

Toate situațiile descrise mai înainte sunt strâns legate de procesele și activitățile-cheie ale companiei, care trebuie să concorde cu obiectivele și strategia acesteia. Astfel, toate obiectivele critice ale afacerii (cum ar fi o modificare a strategiei corporației) trebuie să fie transformate în procese-cheie de conducere pentru toate părțile implicate în afacere în timpul proiectului SDLC.

Riscurile în dezvoltarea oricărui proiect de SI este ca rezultatul final să nu corespundă cerințelor stabilite inițial. Metoda SDLC necesită o verificare a ciclului de viață pe fiecare fază, care să asigure că erorile potențiale sunt corectate din vreme și pe parcurs, nu doar în timpul testului final de acceptare.

Din perspectiva unui auditor SI, o astfel de abordare pe faze ale ciclului de viață, cu puncte specifice de revizie și evaluare, furnizează următoarele **avantaje**:
- influența auditorului SI crește în mod semnificativ când există proceduri formale și ghiduri directoare care identifică fiecare fază a ciclului de viață al SI, în care auditorul SI poate fi implicat;
- auditorul SI poate revedea cele mai relevante zone și faze ale proiectului de dezvoltare a sistemului, raportând în mod independent conducerii asupra adeziunii privind obiectivele planificate și procedurile companiei;
- auditorul SI poate să identifice părți selective ale sistemului în care se poate implica în funcție de îndemânările și abilitățile sale;
- auditorul SI poate furniza o evaluare a metodelor și tehnicilor aplicate în timpul etapelor de dezvoltare ale ciclului de viață al SI.

Majoritatea SI actuale pot fi împărțite în două categorii:
- **centrate pe cerințele organizației** (*Management Information System* – MIS, *Entreprise Resources Planing* – ERP, *Customers Relationship Management* – CRM) pentru dezvoltarea cărora se folosește metoda SDLC;
- **centrate pe cerințele punctuale ale utilizatorilor finali**, pentru care se folosesc metode alternative de dezvoltare.

[3] CISA, p. 145.

Metoda SDLC se bazează pe o abordare sistematică şi secvenţială, care începe cu studiul de fezabilitate şi progresează prin intermediul definirii cerinţelor, proiectării, dezvoltării, implementării şi postimplementării. Seria fazelor şi paşilor definesc scopuri şi activităţi care urmează a fi executate cu asumarea responsabilităţilor, ieşiri aşteptate şi termene de realizare. Această metodă lucrează cel mai bine când cerinţele proiectului sunt stabile şi bine definite.

Tabelul 3.3.1.1. **Descriere generală a fazelor SDLC**

Faze SDLC	**Descriere generală**
Faza 1 - fezabilitatea	Determină beneficiile strategice ale implementării sistemului fie în favoarea productivităţii, fie în evitarea costurilor, identifică şi cuantifică reducerea costurilor induse de noul sistem şi estimează programul de acoperire a costurilor pe care le presupune implementarea sistemului. Mai mult, factorii intangibili, cum ar fi calificarea utilizatorilor şi maturitatea proceselor afacerii, trebuie luaţi, de asemenea, în considerare şi valorificaţi.
Faza 2 – cerinţele	Defineşte problema de rezolvat şi stabileşte cerinţele funcţionale şi calitative ale noului sistem. Aceste cerinţe pot sta la baza proiectării unui nou SI sau pot fi folosite pentru achiziţionarea unui pachet software existent. În ambele cazuri, utilizatorul trebuie să fie implicat în mod activ.
Faza 3a – proiectarea	Ţinând cont de cerinţele definite în faza 2, se stabileşte un nivel de bază al caracteristicilor sistemului şi subsistemelor, modul în care acestea interacţionează şi cum va fi implementat sistemul utilizând facilităţi hardware, software şi de reţea. În general proiectarea include de asemenea specificaţiile de programare şi ale bazei de date, luând în calcul problemele specifice de securitate. În mod suplimentar, se stabileşte un proces formal de control al schimbării, pentru a preveni intrări necontrolate în cadrul procesului de dezvoltare prin apariţia unor cerinţe noi.
Faza 3b – selecţia	Dacă pe baza cerinţelor definite în faza 2 se alege varianta de achiziţionare a unui pachet software existent, atunci se pregăteşte o cerere de ofertă pentru furnizorii de software. În completarea cerinţelor de funcţionare vor exista solicitări operaţionale, de suport şi tehnice, acestea ţinând cont de disponibilitatea financiară a producătorilor şi a proviziilor încredinţate spre păstrare, urmând a fi utilizate în selecţia pachetului de sistem care ar corespunde cel mai bine tuturor cerinţelor organizaţiei.

Faze SDLC	Descriere generală
Faza 4a – dezvoltarea	Folosirea specificațiilor din faza de proiectare pentru a începe procesul operațional de programare și formalizare a proceselor de sistem. În această fază apar de asemenea diferite niveluri de testare pentru a verifica și a valida ceea ce s-a realizat. Această fază va include în general testarea tuturor componentelor sistemului, precum și câteva elemente de testare a identității utilizatorilor.
Faza 4b – configurarea	Configurarea sistemului în cazul în care acesta este un sistem general (pachet) care trebuie să răspundă cerințelor organizației. Aceasta trebuie să fie mai degrabă în concordanță cu parametrii de control ai sistemului decât să presupună schimbarea programului. Pachetele moderne de software sunt parametrizate și extrem de flexibilie, dând posibilitatea ca un astfel de pachet să se potrivească mai multor organizații.
Faza 5 – implementarea	Stabilirea operațiilor noului sistem informatic, după trecerea testelor finale de acceptare de către utilizator. Sistemul poate să treacă printr-un proces de certificare și acreditare pentru evaluarea eficienței aplicațiilor afacerii în scopul diminuării riscului la un nivel corespunzător și al furnizării acelor elemente care să ateste eficacitatea sistemului în vederea îndeplinirii obiectivelor propuse și în stabilirea unui nivel potrivit de control intern.
Faza 6 – postimplementarea	Urmând implementarea cu succes a unui sistem nou, postimplementarea este un proces formal care pune în valoare în ce măsură sistemul și proiectul sunt adecvate din punct de vedere al raportului cost - beneficiu și al recuperării investiției (*Return on Investment* - ROI), având în vedere eventualele abateri constatate. Astfel, managementul pentru utilizatorii finali poate furniza lecții învățate și/sau planuri pentru a notifica deficiențele sistemului, precum și recomandări pentru proiectele viitoare privind dezvoltarea sistemului.

Pentru măsurarea factorilor critici de succes ai proiectului (spre exemplu pentru o aplicație de *e-commerce*) metoda SDLC poate include un set de indicatori cum ar fi: productivitatea, calitatea, valoarea economică, serviciile către client etc. (tabelul 3.3.1.2).

Avantajul principal al unei astfel de abordări este acela că furnizează un cadru metodologic în interiorul căruia pot fi plasate toate cerințele fiecărei faze. Cu toate acestea, pe parcursul derulării procesului apar o serie de probleme, cum ar fi:

- evenimente neanticipate, care pot crea dificultăţi în aplicarea metodei;
- dificultatea de a obţine un set explicit de cerinţe din partea clientului/utilizatorului;
- gestionarea cerinţelor şi dificultatea de a-l convinge pe utilizator referitor la cerinţele la care nu se poate răspunde sau care nu pot fi garantate în funcţionarea unui sistem;
- schimbarea mediului unei afaceri care modifică şi cerinţele clientului/utilizatorului înainte de livrare.

Tabelul 3.3.1.2. **Măsurarea factorilor critici de succes**

Productivitate	Bani cheltuiţi/utilizator Număr de tranzacţii/lună Număr de tranzacţii/utilizator
Calitate	Număr de discrepanţe Număr de dispute Număr de fraude sau întrebuinţări greşite detectate
Valoare economică	Reducerea timpului total de prelucrare Valoarea costurilor de administrare
Serviciu client	Timpul util în care s-a răspuns întrebărilor utilizatorului Frecvenţa de comunicare utilă cu utilizatorul

Foarte multe organizaţii, publice şi private, trec de la grupuri de aplicaţii informatice, care interacţionează între ele, la sisteme integrate pentru managementul resurselor la nivelul unei companii, cunoscute adesea ca *Enterprise Resources Planning* (ERP). Mulţi vânzători de software, în special din Europa şi SUA, s-au concentrat asupra acestei pieţe, oferind pachete cu nume comerciale cum ar fi: SAP, PeopleSoft, ORACLE Financials, SSG (Baan) sau J.D. Edwards, care au câştigat piaţa în defavoarea aplicaţiilor independente.

Achiziţia şi implementarea unui sistem ERP are un impact major asupra modului în care compania face afaceri, asupra mediului de control, a direcţiei tehnologice şi a resurselor interne. Prin implementarea unui asemenea pachet, compania este obligată să îşi schimbe filozofia de conducere, politicile şi proiectele de management la cele incluse în pachetul integrat. De aceea, înainte de a lua o decizie în acest sens, se impune o analiză riguroasă a riscurilor care pot apărea ca urmare a acestei schimbări.

Prioritar, pentru a gira un astfel de proiect global, managementul superior, trebuie să evalueze şi să aprobe toate schimbările din arhitectura sistemului, direcţia tehnologică, strategiile de migrare şi bugetele SI.

Descrierea fazelor tradiționale ale ciclului de dezvoltare a SI (SDLC)

După cum se prezintă în tabelul 3.3.1.1, abordarea tradițională a SDLC se compune din șase faze distincte, fiecare dintre ele cu un set de activități și rezultate definite. Vor fi descrise în detaliu scopul fiecărei faze și relația cu fazele anterioare, cu activitățile generale desfășurate și cu rezultatele așteptate. Se va insista mai ales pe activitatea auditorului, a obiectivelor auditului și a diligențelor întreprinse de auditor.

Faza 1: Studiul de fezabilitate

După ce s-a luat hotărârea să se continue proiectul, se începe o analiză pentru a defini cu claritate necesitățile și a identifica alternativele de abordare a acestora. Analiza de acest tip este cunoscută sub denumirea de *studiu de fezabilitate*.

Un studiu de fezabilitate se ocupă de analiza beneficiilor și a soluțiilor pentru problema identificată. Acesta include dezvoltarea unui studiu de caz, care stabilește beneficiile strategice ale implementării sistemului, fie din punctul de vedere al câștigului de productivitate, fie al evitării unor costuri viitoare; identifică și cuantifică economiile de costuri datorate noului sistem; estimează un program de recuperare a costurilor de implementare a sistemului sau prezintă indicatorii probabili de rentabilitate a investiției. Se pot identifica și eventualele beneficii intangibile, cum ar fi imaginea entității, creșterea încrederii clienților, un moral mai bun etc. În orice caz, beneficiile trebuie să fie cuantificate ori de câte ori acest lucru este posibil.

În cadrul studiului de fezabilitate se abordează, de regulă, următoarele aspecte:

- stabilirea timpului disponibil pentru implementarea soluției cerute;
- determinarea unei soluții alternative optime, bazate pe risc, pentru îndeplinirea cerințelor comerciale, precum și a cerințelor de resurse de informații generale (de exemplu, dacă este mai rentabilă dezvoltarea unui sistem decât achiziționarea lui). Resursele de informații, așa cum sunt definite în COBIT, includ: persoane, aplicații, tehnologii, amenajări și date organizate și gestionate printr-un set dat de procese TI (de exemplu, SDLC, RAD etc. pentru domeniul de achiziție și implementare);
- determinarea în ce măsură un sistem existent poate fi adaptat pentru a elimina deficiențele cu modificări mici, sau chiar fără modificări (de exemplu, *work around*);
- determină în ce măsură există un produs pe piață care poate soluționa problema apărută;
- determină costul aproximativ pentru dezvoltarea unui produs care să corecteze situația;
- determină dacă soluția concordă cu strategia de afaceri.

Factori ce au impact asupra deciziei de a dezvolta sau de a achiziţiona un sistem:

- data când sistemul trebuie să devină funcţional;
- costul dezvoltării sistemului comparativ cu cel al achiziţionării sale;
- resursele, personalul (disponibilitatea şi abilităţile) şi hardware-ul necesare pentru dezvoltarea sistemului sau pentru implementarea unei soluţii achiziţionate de pe piaţă;
- în cazul unei soluţii achiziţionate de pe piaţă, caracteristicile licenţei (de exemplu, reînnoire anuală, permanentă) şi costurile de întreţinere;
- care sunt celelalte sisteme cărora trebuie să li se furnizeze informaţiile, sau ale căror informaţii trebuie folosite; găsirea sistemului achiziţionat de pe piaţă care să poată fi pus în interfaţă cu sistemul existent;
- compatibilitatea cu planurile de afaceri strategice;
- compatibilitatea cu infrastructura TI a organizaţiei;
- posibilele cerinţe viitoare de modificări funcţionale oferite de sistem.

Rezultatul studiului de fezabilitate va trebui să aibă formă de raport comparativ, care include toate alternativele/soluţiile, care prezintă rezultatele criteriilor analizate (de exemplu: costuri, beneficii, riscuri, resurse necesare, impact asupra organizaţiei).

În strânsă legătură cu *studiul de fezabilitate* se va întocmi un *studiu de impact* care analizează efecte viitoare, posibile, ale unui proiect de dezvoltare asupra proiectelor curente şi a resurselor disponibile. Documentul rezultat trebuie să cuprindă argumentele pro şi contra pentru urmarea unei anumite căi.

Faza 2: Definirea cerinţelor

Cerinţele includ o descriere a ceea ce sistemul va trebui să facă, cum vor interacţiona utilizatorii cu sistemul, condiţiile în care va opera sistemul, precum şi criteriile informatice pe care sistemul va trebui să le îndeplinească. Principiile-cadru ale COBIT arată că aceste cerinţe trebuie să includă aspecte asociate cu eficacitatea, eficienţa, confidenţialitatea, integritatea, disponibilitatea, conformitatea şi fiabilitatea sistemului.

Pentru a îndeplini cele de mai sus în faza de definire a cerinţelor, trebuie:

- să se identifice şi să se consulte împuterniciţii pentru a determina care sunt aşteptările lor;
- să se analizeze cerinţele în scopul de a detecta şi a corecta conflictele şi a stabili priorităţile;
- să se identifice legăturile sistemului şi modul în care sistemul va interacţiona cu mediul său;
- să se verifice dacă cerinţele sunt complete, consecvente, neambigue, verificabile, modificabile, testabile, retrasabile. Datorită costurilor ridicate ale rectificării cerinţelor în următoarele faze de dezvoltare, este foarte rentabil să se facă verificări eficace ale cerinţelor;
- să se rezolve conflictele între persoanele cu putere de decizie;
- să se rezolve conflictele între cerinţele impuse şi resursele disponibile.

În acest proces, utilizatorii menționează care este necesarul de resurse de informare, neautomatizate și automatizate, și modul în care aceștia doresc să fie accesate de sistem (de exemplu: controlul accesului, cerințe de reglementare, necesități de management al informației și cerințe de interfață).

Din acest proces preliminar poate fi dezvoltat un proiect preliminar general al sistemului și prezentat managementului utilizatorului pentru analiză, modificări, aprobare și avizare. Ulterior, se face un proiect de planificare în timp a etapelor de dezvoltare, testare și implementare a sistemului. De asemenea, se obțin promisiunile ferme ale dezvoltatorilor sistemului și ale departamentului de utilizatori afectat, de a contribui cu resursele necesare definitivării proiectului.

Un instrument important în crearea unui proiect general preliminar este utilizarea diagramei relațiilor dintre entități (*Entity Relationship Diagram* - ERD), care descrie datele sistemului și modul în care acestea interacționează. Aceasta poate fi folosită ca instrument de analiză a cerințelor, cu scopul de a înțelege care sunt datele pe care sistemul trebuie să le preia și să le administreze, reprezentând un model logic de date.

În această etapă, auditorii SI sunt preocupați să determine dacă au fost definite cerințe de securitate adecvate pentru adresare, confidențialitate, integritate și disponibilitatea sistemului. Tot în această etapă se va stabili dacă au fost definite căi adecvate pentru audit, ca parte a sistemului și măsura în care acestea afectează capacitatea auditorului de a identifica problemele pentru o monitorizare corectă.

Dacă rezultatul hotărârii de a dezvolta/achiziționa este acela de a cumpăra un pachet software oferit de un vânzător, atunci utilizatorul trebuie să fie implicat activ în evaluarea pachetului și în procesul de selecție.

Auditorii SI sunt implicați în procesul de achiziționare a acestui software în scopul de a determina dacă s-a avut în vedere un nivel de securitate adecvat, înainte de încheierea contractului.

Faza 3: Proiectarea

Pe baza proiectului preliminar și a cerințelor utilizatorilor definite în faza de definire a acestora, poate fi dezvoltat un proiect detaliat. În general, se desemnează o echipă de programatori și analiști pentru a defini arhitectura și a schița un plan general al sistemului care să fie ulterior detaliat sau descompus în module și componente. În funcție de complexitatea sistemului, este posibil să fie necesare mai multe iterații pentru definirea specificațiilor la nivel de sistem, de la care să se mărească nivelul de detaliere necesar pentru a porni activitățile de dezvoltare, cum ar fi scrierea programelor.

Implicarea utilizatorului în proiectare

După ce procesele de afaceri au fost documentate şi s-a înţeles cum ar putea fi executate aceste procese în noul sistem, implicarea utilizatorilor în faza de proiectare este limitată. Dată fiind discuţia tehnică ce intervine de obicei în timpul analizării proiectului, participarea utilizatorului final în analiza detaliată a lucrărilor proiectului nu este de obicei convenabilă. Cu toate acestea, echipa de dezvoltare trebuie să explice modul în care arhitectura acestui software va satisface cerinţele sistemului şi să scoată în evidenţă argumentele pentru care au luat anumite decizii de proiectare. Alegerea unei anumite configuraţii hardware şi software poate avea implicaţii asupra costurilor, de care decidenţii trebuie să fie conştienţi, ţinând cont şi de implicaţiile de interes pentru auditorul SI.

Activităţile principale de proiectare includ:

- proiectarea schemei funcţionale a sistemului şi relaţiilor dintre entităţi, în măsură să ilustreze modul în care informaţia va circula prin sistem;
- descrierea intrărilor şi a ieşirilor, cum ar fi machetele de ecran şi de rapoarte. Un instrument de realizare a prototipurilor, se foloseşte cel mai adesea în procesele de proiectare a ecranului şi de prezentare, prin facilităţi de programare on-line, ca parte a unui mediu de dezvoltare integrat;
- determinarea paşilor de prelucrare şi a regulilor de calcul;
- determinarea structurii fişierelor;
- întocmirea specificaţiilor de program pe baza cerinţelor stabilite în etape anterioare;
- proiectarea planurilor de testări pentru diferite niveluri: unitate (program), subsistem (modul), integrare (sistem), interfaţa cu alte sisteme, încărcarea şi iniţializarea fişierelor, securitatea, copii de siguranţă (*backup*) şi recuperare (*recovery*);
- stabilirea planurilor de conversie a datelor şi a procedurilor manuale, pentru trecerea de la sistemul vechi la cel nou. Planurile detaliate de conversie vor diminua dificultăţile de implementare care apar din cauza datelor incompatibile, resurselor insuficiente sau personalului care nu este familiarizat cu operarea noului sistem.

Software baselining

Termenul de *software baseline* reprezintă punctul dincolo de care nu se mai admit modificări decât în urma unei proceduri aprobate. Cerinţele utilizatorului sunt analizate una câte una şi evaluate din punct de vedere al timpului şi al costurilor. Schimbările se fac după luarea în considerare a diverselor riscuri, dar nu înainte de a trece printr-o procedură precisă şi strictă de aprobare, pe baza unei analize de impact costuri-beneficii. O tratare neadecvată a cerinţelor pentru un sistem, prin procesul de *baselining*, poate avea ca rezultat o serie de riscuri. Cel mai mare risc este cel numit *scope creep*, un proces de schimbare a cerinţelor în cursul dezvoltării proiectului.

Studii empirice au arătat că, pe parcursul dezvoltării unui proiect, pot apărea până la 25% schimbări de cerințe, ceea ce duce la creșterea eforturilor și a costurilor de dezvoltare.

Termenul de *software baseline* se referă și la punctul în care apare procesul de stabilire formală a configurației software. În acest punct, produsele rezultate din activitatea de dezvoltare a unui software sunt denumite *configurații baseline* și primesc numere de versiune. Aici se includ, de exemplu, cerințele funcționale, specificațiile și planurile de testare. Toate aceste produse din procesul de lucru sunt elemente de configurare și sunt identificate și supuse unui control formal al modificărilor din partea managementului. Acest proces va fi folosit pe toată durata ciclului de viață al sistemului, în care procedurile pentru ciclul de elaborare a aplicațiilor software, privitoare la analiză, proiectare, dezvoltare, testare și desfășurare, vor fi impuse prin noi cerințe sau prin modificări ale cerințelor existente.

După ce a fost terminat proiectul detaliat și au fost obținute inclusiv aprobările utilizatorilor, după stabilirea formală a configurației software, acesta se predă echipei de dezvoltare pentru scrierea programelor.

Implicarea auditorului SI

Implicarea auditorului SI este orientată în special spre aspecte care au în vedere în ce măsură, în specificațiile sistemului și ale planurilor de testare, este incorporat un set adecvat de controale sau în ce măsură în sistem sunt implementate funcții de auditare continuă on-line (în special pentru aplicațiile de comerț electronic și alte tipuri de medii care lucrează fără hârtie). În plus, auditorul SI este interesat de evaluarea eficacității procesului de proiectare, a tehnicilor de proiectare structurate, de elaborarea de prototipuri și planuri de testare, de stabilirea formală a configurației software, de stabilirea unui proces formal de modificări al acestui software, care să nu permită includerea oricăror schimbări în cerințele de sistem, fără un proces formal de analiză și aprobare.

Principalele documente care rezultă din această fază includ specificațiile pentru sistem, subsistem, program și baza de date, planurile de testare și un proces formal și documentat de control al schimbărilor aduse ulterior sistemului.

Faza 4: Dezvoltarea

În această fază, răspunderea revine în primul rând programatorilor și analiștilor de aplicații care dezvoltă sistemul. Într-un mediu de testare/dezvoltare, principalele activități desfășurate sunt următoarele:

- codificarea și dezvoltarea programelor și a documentelor;
- dezvoltarea de programe de depanare și testare;
- dezvoltarea de programe de conversie a datelor din sistemul vechi pentru a fi folosite de sistemul nou;

- crearea de proceduri-utilizator pentru a dirija tranziţia către noul sistem;
- instruirea utilizatorilor pentru folosirea noului sistem;
- preocuparea pentru ca modificările să fie documentate şi aplicate cu acurateţe şi în totalitate la software-ul achiziţionat de la vânzător, pentru a exista garanţia ca viitoarele versiuni modernizate ale codului să fie aplicabile.

Metode şi tehnici de programare

Aplicarea standardelor de programare reprezintă un element esenţial în dezvoltarea unui SI, deoarece servesc ca metodă de comunicare atât între membrii echipei de programare, cât şi între echipă şi utilizatori. Acestea minimizează întârzierile în programare cauzate de fluctuaţia de personal, asigură materialul necesar sistemului pentru a fi eficace, permit întreţinerea ulterioară a programului.

În plus, tehnicile tradiţionale de programare structurată ar trebui aplicate pentru dezvoltarea de produse software care să fie nu numai de calitate, dar şi uşor de întreţinut. Ca şi în cazul specificaţiilor de proiectare, aplicaţiile care utilizează programarea structurată sunt mai uşor de dezvoltat, de înţeles şi de întreţinut, deoarece sunt divizate pe subsisteme, componente, module, programe, subrutine şi unităţi. În general, cu cât fiecare element software descris execută o singură funcţie dedicată (coeziune) şi îşi menţine independenţa faţă de alte elemente comparabile (cuplare), cu atât va fi mai uşor de întreţinut şi de perfecţionat sistemul, întrucât este mai uşor de stabilit unde şi cum trebuie să se facă o modificare.

Posibilităţile de programare on-line (mediul de dezvoltare integrat)

Pentru a uşura utilizarea eficace a metodelor şi tehnicilor de programare structurată, trebuie folosit un sistem de programare on-line, ca parte a unui mediu de dezvoltare integrat care include un server şi instrumente adecvate ce permit programatorilor editarea şi compilarea interactivă a programelor de la un terminal sau de la o staţie de lucru.

În general, o facilitate de programare on-line permite o dezvoltare mai rapidă a programelor şi aplicarea de standarde şi tehnici de programare structurate. Ea îmbunătăţeşte şi abilităţile programatorului în a rezolva probleme. Totuşi, sistemele on-line pot genera erorile ca urmare a accesului neautorizat. Se poate folosi un software de control al accesului, reducând acest risc.

Astăzi, facilităţile de programare on-line se folosesc pe staţiile de lucru PC. Biblioteca de programe se află pe un server, ca şi sistem de management al unei *mainframe library*, dar modificările/dezvoltarea şi testarea se fac pe staţia de lucru. Această abordare poate micşora costurile de dezvoltare, permite timpi scurţi de răspuns şi extinde resursele şi mijloacele ajutătoare de programare (de exemplu, unelte de editare, limbaje de programare, mijloace de depanare). Din perspectiva controlului, această abordare introduce un potenţial punct slab prin:

- proliferarea unor versiuni multiple ale programelor;
- reducerea integrității programului și a prelucrării, prin potențialul crescut al accesului și aducerilor la zi neautorizate;
- posibilitatea ca modificări valide să fie suprascrise de alte modificări.

Depanarea programelor

Multe erori de programare (*bug*-uri) sunt detectate în cursul procesului de dezvoltare a sistemului, după ce programatorul rulează un program într-un mediu de testare. Scopul depanării programelor în cursul procesului de dezvoltare a sistemului este de a asigura ca toate întreruperile anormale ale programului (*abend*) și erorile din programul sursă să fie detectate și corectate înainte ca programul, în forma sa finală, să intre în producție.

Un instrument de depanare de programe este un program care îl ajută pe programator să depisteze eventualele erori și apoi să le corecteze. Compilatoarele îi pot oferi un *feedback* programatorului, dar ele nu sunt considerate instrumente de depanare de programe. **Instrumentele de depanare a programelor se împart în trei categorii principale:**

- monitoare logice (*logic path monitor*), care raportează secvențele de evenimente executate de program, în felul acesta dând indicii programatorului despre erorile de logică;.
- vidajul memoriei (*memory dumps*), care asigură o imagine a conținutului memoriei interne la un moment dat. Acest lucru se face adesea atunci când programul se întrerupe, oferindu-i programatorului indicii despre incoerențe în date sau valorile parametrilor. O variantă de urmărire (*trace*) va face același lucru în etape diferite ale rulării programului, pentru a arăta evoluția unor locații de memorie internă sau regiștri;
- analizoare de ieșire (*output analyzer*), care ajută la verificarea acurateței rezultatelor rulării programului. Aceasta se realizează prin compararea rezultatelor așteptate cu rezultatele reale.

Testarea

Testarea este un element esențial al procesului de dezvoltare care verifică și validează faptul că programul, subsistemele sau aplicațiile îndeplinesc funcțiile pentru care au fost proiectate. Testarea determină și în ce măsură unitățile testate operează fără defecțiuni de funcționare sau efecte adverse asupra altor componente ale sistemului.

Varietatea de metode de dezvoltare și de cerințe ale organizațiilor asigură o gamă largă de scheme sau niveluri de testare. Fiecare set de teste se realizează cu un set de date diferit și sub răspunderea altor persoane sau funcții. **Auditorul SI poate juca un rol de prevenție sau poate ajuta la identificarea erorilor în procesul de testare.**

Elementele unui proces de testare software

Pentru a dirija procesul de testare şi a ajuta ca toate componentele sistemului să funcţioneze conform aşteptărilor, au fost definite **elementele de bază pentru activităţile de testare a aplicaţiilor software, în care se includ următoarele**:

✓ **planuri de testare,** dezvoltate la începutul ciclului de viaţă şi rafinate până la faza de testare reală, identifică porţiuni specifice ale sistemului de testat. Acestea pot specifica şi nivelul de gravitate a problemelor sesizate. Persoana care face testările determină severitatea problemei sesizate în cursul testării şi stabileşte dacă problema poate fi reparată sau rămâne în starea iniţială. Adesea, problemele legate de interfaţă sunt considerate ca fiind de importanţă mai scăzută şi pot fi lăsate nesoluţionate în situaţia în care problema timpului devine stringentă pentru managerul de proiect. Finanţatorul proiectului, managementul utilizatorului final şi managerul de proiect stabilesc la începutul fazei de testare tipurile de deficienţe pe grade de severitate. Planurile de testare includ şi abordările de testare:

- **de jos în sus** (*bottom-up*) începe cu testarea modulelor şi continuă prin integrarea componentelor de jos în sus, până ce are loc o testare a sistemului în ansamblul său. Avantajele metodei constau în faptul că:
  - nu sunt necesare programe intermediare de legătură sau fragmente de simulare (*stubs*) şi nici drivere;
  - se poate începe testarea înainte de terminarea tuturor programelor;
  - erorile severe din modulele sunt depistate devreme;
- **de sus în jos** (*top-down*) urmează calea inversă. Avantajele metodei sunt:
  - testarea funcţiilor şi a proceselor majore se face din timp;
  - erorile de interfaţă sunt detectate din timp;
  - creşte încrederea în sistem, deoarece programatorii şi utilizatorii văd un sistem care funcţionează.

În general, majoritatea testărilor sistemelor mari urmează abordarea de la particular la global (*bottom-up*), care implică mai multe niveluri de testare.

✓ **executarea testării şi raportarea rezultatelor acesteia** descriu resursele necesare pentru testare, inclusiv personalul implicat şi resursele/facilităţile informatice folosite pe durata testului, precum şi rezultatele reale faţă de cele anticipate. Rezultatele raportate, împreună cu planul de testare, vor trebui să fie păstrate ca parte a documentaţiei permanente a sistemului;

✓ **abordarea problemelor încă nerezolvate** identifică erorile şi neregulile din testele executate. Dacă apar astfel de probleme, respectivul test trebuie reproiectat în cadrul planului de testare, până ce se obţin condiţii acceptabile şi testele pot fi refăcute.

Clasificarea testărilor

Din mecanismele complete de testare, vor fi utilizate testele considerate adecvate în funcţie de dimensiunea şi complexitatea sistemului realizat:

- ✓ **testarea unităţii** (*unit testing*) - testarea unui program sau modul individual. Foloseşte un set de cazuri de testare care se concentrează pe controlul structurii procedurale a programului. Aceste teste verifică dacă operaţiile interne ale programului sunt în concordanţă cu specificaţiile iniţiale;
- ✓ **testarea interfeţei sau integrării** (*interface or integration testing*) - un test hardware sau software care evaluează conectarea a două sau mai multe componente (module) care transmit informaţii de la una la alta. Obiectivul constă în cuplarea modulelor testate unitar şi construirea unei structuri integrate, în conformitate cu proiectul;
- ✓ **testarea sistemului** (*system testing*) constă într-o serie de teste, concepute pentru a asigura că programele, obiectele, schemele de baze de date etc. formează împreună un sistem nou sau modificat şi funcţionează corect. Aceste proceduri de testare sunt adesea realizate într-un mediu diferit de producţie, testare şi dezvoltare, de către personalul de dezvoltare desemnat ca „echipă de testare". În cursul testării sistemului, pot fi executate următoarele analize:
  - **testarea recuperării** (*recovering testing*) - verificarea abilităţii sistemului de a se recupera după o defecţiune software sau hardware;
  - **testarea securităţii** (*security testing*) - verificarea dacă sistemele modificate sau cele noi includ măsuri adecvate de control şi acces şi nu introduc nicio breşă în securitate care ar putea compromite alte sisteme;
  - **testarea de volum** (*volume testing*) - studierea impactului asupra aplicaţiei cu un volum de înregistrări crescut, pentru a determina volumul maxim de înregistrări (date) pe care aplicaţia le poate prelucra;
  - **testarea de stres** (*stress testing*) - studierea impactului asupra aplicaţiei prin testarea cu un număr crescut de utilizatori/servicii concurente care accesează aplicaţia, spre a determina numărul maxim de utilizatori/servicii concurente pe care îi/le poate prelucra aplicaţia;
  - **testarea de performanţă** (*performance testing*) - compararea performanţelor sistemului cu cele ale altor sisteme echivalente, folosind elemente de analiză comparativă (*benchmark*) bine definite.
- ✓ **testarea pentru acceptarea finală** (*final acceptance testing*). Dacă echipa responsabilă de sistem consideră că testele iniţiale şi/sau de

sistem s-au realizat cu succes, sistemul modificat este gata pentru testarea/acceptarea finală, care are loc în faza de implementare. În timpul acestei faze, metodele de testare definite pentru a fi aplicate vor trebui încorporate în metodologia de asigurare a calităţii adoptate de organizaţie. Activităţile de asigurare a calităţii trebuie să controleze situaţia, astfel încât, cele mai adecvate niveluri de testare să fie aplicate la toate proiectele de dezvoltare de software. Testarea pentru acceptarea finală constă în două componente majore:

- testarea pentru asigurarea calităţii (*Quality Acceptance Testing* - QAT), care se focalizează pe aspectele tehnice ale aplicaţiei, şi
- testarea acceptării de către utilizator (*User Acceptance Testing* - UAT), care se focalizează pe aspectele funcţionale ale aplicaţiei.

Cele două tipuri de testări, QAT şi UAT, au obiective diferite, prin urmare nu trebuie combinate.

Testarea pentru asigurarea calităţii (QAT) se focalizează pe specificaţiile documentate şi pe tehnologia folosită, însă nu şi pe testarea funcţionalităţii. Acest tip de testare verifică în ce măsură SI proiectat lucrează documentat, prin testarea proiectului logic şi a tehnologiei însăşi. De asemenea, verifică dacă au fost respectate specificaţiile tehnice documentate şi setul de cerinţe de livrare (*deliverables*). QAT se realizează în special de departamentul SI, participarea utilizatorului final fiind minimă şi la cererea acestuia.

Testarea acceptării de către utilizator (UAT) verifică dacă sistemul este gata pentru exploatare şi dacă satisface toate cerinţele iniţiale. Această testare include următoarele etape:

- definirea de strategii şi proceduri de testare;
- proiectarea de cazuri şi scenarii de testare;
- executarea testărilor;
- utilizarea rezultatelor pentru a verifica starea de pregătire a sistemului.

După terminarea testului de acceptare finală, ultimul pas este procesul de certificare şi acreditare, care include: evaluarea documentaţiei şi eficacitatea testării, evaluarea planului de securitate, revizuirea planului de securitate, a controalelor de securitate. În această etapă sunt implicaţi proprietarul sistemului şi personalul care se ocupă de securitatea sistemului.

În final, după terminarea testărilor, auditorul SI trebuie să emită o opinie pentru management, dacă sistemul poate sau nu să intre în producţie. Acest raport trebuie să specifice deficienţele care urmează să fie corectate în sistem, să identifice şi să explice riscurile pe care şi le asumă organizaţia prin implementarea noului sistem.

Alte tipuri de testări includ:

- ✓ **testarea alfa și beta** (*alpha and beta testing*) – este posibil ca o primă versiune a aplicației (sau a produsului software) să nu conțină toate detaliile planificate pentru versiunea finală. În mod obișnuit, un software, înainte de a fi considerat terminat, trece prin două etape de testare.
  - Prima etapă, denumită *testare alfa,* se realizează adesea numai de utilizatori, în cadrul organizației care dezvoltă acel software (de exemplu, testarea sistemelor).
  - A doua etapă, denumită *testare beta,* este o formă de testare a acceptării de către utilizator și, de obicei, implică un număr limitat de utilizatori externi. Testarea beta este ultima etapă de testare și, în mod normal, implică trimiterea produsului la locații de testare beta din afara mediului de dezvoltare, pentru expunere la lumea reală.
- ✓ **Testarea-pilot** (*pilot testing*) – este o testare preliminară, care se focalizează pe aspecte specifice predeterminate ale sistemului. Nu este concepută pentru a înlocui alte metode de testare, trebuie doar să asigure o evaluare limitată a sistemului;
- ✓ **testarea structurală** (*white box testing*) – evaluează eficacitatea logicii programului software și se bazează pe cunoașterea modului în care ar trebui să funcționeze programul. Practic, datele de testare sunt folosite pentru a determina acuratețea procedurală sau condițiile unei căi logice a programului (de exemplu, este aplicabilă testării unității și integrării). Totuși, testarea tuturor căilor logice posibile în sisteme informatice mari nu este fezabilă mai ales din cauza costurilor prohibitive, motiv pentru care se folosește numai pe o bază de selecție;
- ✓ **testarea specificațiilor** (*black box testing*) – este o formă de testare a integrității, asociată cu testarea eficacității de operare funcțională a componentelor unui sistem informatic, indiferent de structura internă a programului. Este aplicabilă la procesele de testare ale integrării (interfață) și acceptării de către utilizator;
- ✓ **testarea funcțiunii/validării** (*function/validation testing*) – este similară cu testarea sistemului, dar adesea este folosită pentru a testa funcționalitatea sistemului comparativ cu cerințele, pentru a verifica în ce măsură software-ul construit corespunde solicitărilor clientului;
- ✓ **testarea regresivă** (*regression testing*) – reprezintă procesul de a rula din nou o porțiune a unui scenariu de test sau plan de testare, pentru a verifica în ce măsură modificările sau corecțiile efectuate nu au introdus erori noi. Datele folosite la testarea regresivă trebuie să fie aceleași date care au fost folosite la testarea inițială;

✓ **testarea paralelă** (*parallel testing*) – este procesul de introducere a datelor de testare în două sisteme - sistemul modificat şi un sistem alternativ (eventual sistemul original), urmând a compara ulterior rezultatele;

✓ **testarea de sociabilitate** (*sociability testing*) – scopul acestor teste este de a confirma că sistemul nou sau modificat poate opera în mediul său ţintă fără a avea un impact negativ asupra sistemelor existente. Aceasta nu se referă numai la platforma pe care va rula aplicaţia principală şi interfeţele cu celelalte sisteme, ci şi la modificările aduse mediului desktop în server sau de dezvoltare web. Pe calculatorul utilizatorului pot rula multe aplicaţii, posibil şi simultan, astfel că este important să se testeze impactul instalării unor noi biblioteci cu legare dinamică (DLL) care fac modificări în regiştrii de sistem sau în fişierele de configurare şi care pot utiliza inclusiv memorie suplimentară.

Faza 5: Implementarea

După o testare cu succes a întregului sistem, acesta este pregătit să migreze în mediul de exploatare curentă. Programele au fost testate şi rafinate; procedurile programului şi termenele de producţie sunt fixate; toate datele necesare au fost convertite cu succes şi încărcate în noul sistem; utilizatorii au dezvoltat proceduri şi au fost instruiţi pentru utilizarea noului sistem. S-a stabilit o dată pentru migrarea sistemului, astfel încât utilizarea acestuia poate începe.

Planificarea implementării trebuie să înceapă cu mult înainte de data implementării, iar planul oficial de implementare trebuie conceput încă din faza de proiectare, urmând a fi revizuit pe măsură ce proiectarea înaintează. Fiecare pas în pregătirea mediului de utilizare trebuie să fie bine precizat, inclusiv modul de verificare a aceastei etape, care este procedura de revenire la situaţia anterioară în cazul în care apar probleme, cine poartă răspunderea în astfel de situaţii. În cazul în care noul sistem va fi o interfaţă pentru alte sisteme, sau dacă acesta va fi distribuit pe mai multe platforme, este de dorit să se facă un set suplimentar de teste finale, de punere în funcţiune în mediul de producţie, pentru a verifica conectivitatea de la un capăt la celălalt. Dacă se derulează astfel de teste, va trebui avută grijă ca tranzacţiile de test să nu rămână în bazele de date sau în fişierele de producţie.

În cazul unui software achiziţionat, proiectul de implementare ar putea fi coordonat de managementul utilizatorului, cu ajutorul managementului SI, dacă este necesar. Întregul proces nu trebuie delegat vânzătorului, deoarece angajaţii/reprezentanţii săi ar putea face unele modificări neautorizate.

O conversie de date la scară mare poate deveni la rândul ei un proiect în cadrul unui alt proiect, deoarece necesită un volum apreciabil de analiză, proiectare şi planificare. Unii dintre paşii necesari pentru o conversie de succes a datelor ar putea consta în:

- determinarea, după caz, a datelor care trebuie convertite prin program;
- curățarea prealabilă a datelor înainte de conversie;
- identificarea metodelor care trebuie să fie folosite pentru a verifica conversia, cum ar fi compararea automată a fişierelor, compararea contorului de înregistrări ale fişierelor cu totalurile de control, compararea balanțelor contabile şi compararea datelor individuale pe bază de eşantioane;
- stabilirea de parametri pentru o conversie de succes. De exemplu, este necesar să existe o concordanță de 100% între vechiul şi noul sistem, sau va fi acceptabilă o oarecare diferență, în limite prestabilite?;
- planificarea calendaristică a etapelor de conversie;
- proiectarea de rapoarte care să documenteze conversia, inclusiv construirea datelor şi transformările acestora.;
- proiectarea de rapoarte care să documenteze excepțiile, adică orice element care nu poate fi convertit automat;
- stabilirea de răspunderi pentru verificarea, semnarea de încheiere a paşilor individuali de conversie şi de acceptare a întregii conversii. În mod uzual, aceasta este responsabilitatea proprietarului sistemului;
- dezvoltarea şi testarea unor programe de conversie, funcționale şi performante;
- realizarea uneia sau chiar a mai multor simulări de conversie, pentru a familiariza personalul cu secvențele de evenimente şi cu rolul pe care îl joacă, şi pentru a testa procesul de conversie integral, cu date reale;
- rularea conversiei finale se va face cu personalul personalul stabilit pentru acest proces.

Externalizarea procesului de conversie este şi ea posibilă, cu încheierea unui contract de confidențialitate.

După ce s-au stabilit operațiunile, pasul următor este *testarea de acceptare*, care reprezintă o testare completă a sistemului, în mediul în care va opera. Prin această testare, se confirmă faptul că sistemul proiectat corespunde cerințelor formulate şi poate intra în utilizare curentă.

După parcurgerea testului de acceptare din partea utilizatorilor, are loc trecerea de la sistemul existent la cel nou, cunoscută sub unele de desprindere (*cutover* sau *go-live*).

Trecerea la noul sistem se poate realiza în trei moduri diferite:

Trecerea paralelă (*parallel changeover*)
Această tehnică include, pe axa timpului, rularea sistemului nou, apoi rularea atât a celui vechi, cât şi a celui nou, în paralel şi, în final, trecerea integrală la sistemul nou, după ce se câştigă încredere în modul în care acesta funcționează. Printr-o astfel de abordare, utilizatorii vor trebui să folosească ambele sisteme în perioada de

suprapunere. Aceasta va minimiza riscul utilizării noului sistem şi, în acelaşi timp, va ajuta la identificarea problemelor pe care le pot întâlni utilizatorii la începutul lucrului cu noul sistem. După o perioadă de suprapunere, utilizatorul începe să aibă încredere şi certitudinea că se poate baza pe noul sistem. În acest moment, se întrerupe folosirea vechiului sistem, iar noul sistem devine operaţional în totalitate.

Trecerea în etape (*phased changeover*)
Cu această abordare, sistemul vechi este defalcat în module livrabile. Iniţial, se elimină primul modul al vechiului sistem şi se pune în funcţiune primul modul al noului sistem. Apoi se elimină al doilea modul al vechiului sistem şi se pune în funcţiune al doilea modul al noului sistem. Se procedează aşa în continuare până se ajunge la ultimul modul.

Trecerea abruptă (*abrupt changeover*)
Cu această abordare, sistemul nou ia locul sistemului vechi la o dată de şi la o oră stabilită pentru întreruperea sistemului vechi, moment în care sistemul vechi se opreşte şi sistemul nou îi ia locul.

Concluzionând, trecerea la noul sistem include patru etape, sau activităţi majore:
- conversia fişierelor şi programelor, testarea pe un banc de probă;
- instalarea noului hardware, a sistemului de operare, a sistemului de aplicaţii şi a datelor migrate;
- instruirea pe grupuri a angajaţilor sau a utilizatorilor;
- planificarea operaţiilor şi rularea testelor pentru momentul de salt sau de trecere la exploatarea noului sistem.

Printre riscurile ce pot apărea în procesul de trecere se numără următoarele: afectări ale protecţiei activelor, a integrităţii datelor, eficacităţii sistemului, eficienţei sistemului.

Faza 6: Analiza postimplementare
În urma implementării cu succes a noului sistem, este bine să se verifice în ce măsură acesta a fost corect proiectat şi dezvoltat şi dacă au fost implementate controalele necesare. Pentru aceasta, **o analiză postimplementare ar trebui să îndeplinească următoarele obiective:**
- evaluează caracterul adecvat al sistemului:
    - îndeplineşte sistemul obiectivele cerinţelor utilizatorului?
    - au fost definite şi implementate corect controalele de acces?
- evaluează măsurătorile care au stabilit raportul dintre costuri şi beneficii sau rentabilitatea investiţiei;
- dezvoltă recomandări care au în vedere neadecvările şi deficienţele sistemului;

- dezvoltă un plan de implementare a recomandărilor;
- evaluează procesul de dezvoltare a proiectului:
  - au fost urmate metodologiile, standardele și tehnicile alese?
  - au fost adecvate tehnicile de gestionare a proiectului care au fost aplicate?

Este important de notat că, pentru ca o analiză postimplementare să fie eficace, informațiile care trebuie analizate trebuie să fie identificate și reținute încă din faza de pornire a proiectului, urmând a fi colectate la fiecare etapă a proiectului. De exemplu, managerul de proiect ar putea stabili anumite puncte de control pentru a măsura eficacitatea proceselor software și acuratețea estimării pachetelor de software pe durata executării proiectului.

O **analiză postproiectare** se va executa în colaborare cu echipa de dezvoltare a proiectului și cu utilizatorii finali adecvați. De obicei, această analiză internă se concentrează pe evaluarea procesului de executare a proiectului, în timp ce o analiză postimplementare are ca obiectiv evaluarea și măsurarea valorii pe care o are proiectul pentru afacere (realizarea afacerii).

Ca alternativă, se poate realiza o **analiză postimplementare** de către un grup independent, neimplicat în implementarea proiectului (audit intern sau extern). Auditorii SI care fac această analiză trebuie să fie independenți de procesul de dezvoltare a sistemului. De aceea, auditorii SI implicați în consultanță pentru echipa de proiect care a dezvoltat sistemul nu trebuie să realizeze această analiză. Spre deosebire de analiza internă a echipei de proiect, analiza postimplementare, realizată de auditori SI, are tendința să se concentreze pe aspecte legate de controalele dezvoltării sistemului și ale procesului de implementare.

Este important ca orice implicare a auditului în proiectul de dezvoltare să fie atent documentată în documentele de audit, care înregistrează cele găsite de auditorul SI și recomandările acestuia. Acest raport de audit și documentația sa trebuie să fie refolosite pe timpul întreținerii și a modificării, pentru a valida, verifica și testa impactul oricăror modificări făcute sistemului. Sistemul ar trebui supus periodic unei revizuiri, care să certifice atât faptul că acesta este în continuare apt să îndeplinească în mod rentabil obiectivele de afaceri, cât și faptul că s-a păstrat integritatea controlului.

3.3.2. Riscurile asociate dezvoltării SI

Auditorul SI trebuie să fie convins că, numai urmând abordarea managementului SDLC, aceasta nu asigură succesul complet al dezvoltării proiectului. Auditorul SI trebuie să revadă rigoarea procesului de management al proiectului, acordând atenția cuvenită următoarelor elemente:

- întâlnirile în cadrul proiectului privind scopurile şi obiectivele comune;
- planificarea proiectului, incluzând estimările efective de resurse şi timp;
- controlul situaţiilor în care nu există trasate liniile de bază ale software-ului, însemnând că cerinţele noi pot fi adăugate în proiectul software şi dezvoltarea nu mai poate fi controlată;
- urmărirea acţiunilor întreprinse de management pe parcurul proiectării software-ului şi a dezvoltării acestuia;
- revizii şi analize de risc periodice în fiecare fază a proiectului.

Statisticile actuale apreciază că rata de eşec în dezvoltarea SI este de aproximativ 80-85%, ceea ce înseamnă că această activitate este supusă unor riscuri majore care trebuie cunoscute, analizate şi minimizate. Depăşirea uneori foarte mare a costurilor iniţiale, depăşirea cu mai multe luni a termenelor prevăzute pentru finalizarea proiectului, realizarea de sisteme care nu corespund specificaţiilor iniţiale sunt situaţii destul de frecvente.

Dintre cele mai frecvente tipuri de riscuri, se pot aminti:

Riscuri legate de programarea în timp au drept consecinţă nerespectarea termenelor prevăzute. Nivelul riscului este mare atunci când programarea este făcută ţinând cont de cererile formulate de client. O programare bazată pe analiza detaliată a tuturor aspectelor proiectului, a scopului sistemului şi a concepţiei globale diminuează foarte mult acest risc, fără însă a-l exclude în totalitate. Soluţia unei programări bazate pe o examinare prealabilă, făcută în absenţa analizei detaliate, conduce la un risc de nivel mediu.

Riscurile legate de resurse (insuficienţa fondurilor sau lipsa oricărora dintre elementele necesare pentru realizarea proiectului) pot conduce la eşecul întregului proiect. Consecinţele riscului depind de limitările impuse fondurilor băneşti alocate. Astfel, dacă acestea sunt foarte restrictive, riscul este ridicat. Invers, suficienţa fondurilor diminuează riscurile datorate acestui factor.

Aşteptările clientului pot constitui un factor de risc, care se manifestă mai ales în privinţa unor facilităţi şi avantaje care vor fi induse de sistem, o uşurare a muncii şi o creştere a beneficiilor. Dacă aceste obiective nu vor fi riguros stabilite şi măsurabile, riscul specific aşteptărilor clientului va creşte.

Schimbările în procedurile de lucru ale clientului pot constitui un factor de risc important, dacă personalul implicat nu le acceptă. Menţinerea, pe cât este posibil, a procedurilor actuale, însoţite de o bună instruire a utilizatorilor, poate diminua nivelul de gravitate al acestui tip de risc.

Lipsa de consens la nivelul conducerii și a utilizatorilor direcți asupra obiectivelor sistemului constituie un alt factor de risc. Gravitatea sa depinde de importanța deținută de elementele contestate sau neagreate. Astfel, dacă există consens asupra problemelor critice, diferendele referindu-se la elementele secundare, atunci riscul poate fi apreciat drept mediu; în caz contrar, riscul va fi ridicat.

Managementul riscurilor privind proiectele de dezvoltare a SI presupune următoarele acțiuni:
- identificarea tuturor surselor posibile de risc;
- încadrarea într-o clasă de risc (ridicat, mediu, redus);
- elaborarea unui plan de minimizare a riscurilor, având în vedere gradul și posibilitățile de producere a acestora;
- urmărirea și controlul permanent al fiecăruia dintre riscurile identificate;
- readaptarea permanentă a planului de control al riscurilor în funcție de evoluția situației reale.

Pe lângă metoda tradițională, SDLC de dezvoltare a SI există o altă metodă, numită „Analiza, proiectarea și dezvoltarea structurată", care prezintă datele și prelucrările prin intermediul unor diagrame ce permit o abstractizare progresivă, până la un nivel în care se poate trece la programarea SI. Utilizând această metodă, definirea cerințelor unui sistem nou cuprinde următoarele activități:
- diagrame de context în dezvoltarea sistemului (scheme de nivel înalt al procesului afacerii);
- descompunerea ierarhică a fluxurilor de date și de control;
- dezvoltarea controlului transformărilor;
- dezvoltarea minispecificațiilor;
- dezvoltarea dicționarelor de date;
- definirea tuturor evenimentelor externe;
- definirea transformărilor simple ale diagramelor fluxurilor de date pentru fiecare eveniment extern.

Următorul nivel furnizează mai multe detalii în construirea sistemului, incluzând diagramele de dezvoltare a sistemelor, prelucrările fișierelor de date sau specificații ale bazelor de date. Această metodă reprezintă prelucrările într-o manieră modulară *top-down*, permițând programatorilor să dezvolte și să testeze în mod sistematic modulele într-o manieră ierarhică.

3.3.3. Metode de dezvoltare alternativă a SI

În momentul creșterii complexității sistemului și a necesității implementării rapide de noi sisteme, pentru a obține beneficii înaintea schimbării afacerii, producătorii de software au pus bazele strategiilor de dezvoltare alternativă pentru a reduce timpul și costul de întreținere, sau pentru a îmbunătăți calitatea software-ului.
Un auditor SI trebuie să înțeleagă principalele etape și activități aferente acestora în cazul utilizării unor abordări diferite de SDLC.

Principalele abordări de dezvoltare a SI, diferite de abordarea treadițională SDLC, sunt:

- **dezvoltarea incrementală sau progresivă** – sistemul este construit în etape, pe module care, pe măsură ce sunt realizate, sunt livrate. Aceste „livrări" separate sunt adesea realizate ca subproiecte discrete. Practica uzuală este de a livra arhitectura sistemului de bază de la început. Componentele lansate ulterior, se integrează în funcționalitatea sistemului în funcție de rangul utilizatorilor sau locațiile de utilizare;
- **dezvoltarea iterativă** implică construirea sistemului prin iterații şi incrementări succesive, cu posibilități de revenire după fiecare fază de incrementare, pentru a facilita orice ajustare necesară în planul proiectului sau în produsele de dezvoltare software. Dezvoltarea iterativă este privită acum ca cea mai bună practică pentru a face față complexității şi riscurilor asociate proiectelor de dezvoltare software. Gradele de complexitate includ: dimensiunea şi scopul noului sistem dezvoltat (e-business, procesarea tranzacțiilor on-line şi procesarea analitică on-line), rata schimbării afacerii, care creşte gradul de instabilitate; diverse decizii arhitecturale care trebuie să fie luate (Ce firewall să fie utilizat? Ce server WEB să fie utilizat? Să fie utilizată o aplicație server? Ce DBMS să fie utilizat? Ce comunicații şi protocoale de definire a datelor trebuie folosită?); necesitatea de a integra sisteme noi în anumite cazuri, cu sisteme moştenite.

Abordarea de dezvoltare iterativă are un număr de variante:

- **dezvoltarea evolutivă,** care presupune realizarea unui prototip care să fie folosit pentru a verifica cerințele şi a explora rezultatele proiectului. În ultimă instanță, prototipul urmează să fie îmbunătățit, astfel încât să poată fi implementat în producție. În caz contrar, sistemul trebuie reprogramat pe baza concluziilor furnizate de prototip;
- **dezvoltarea în spirală** presupune realizarea unei serii de prototipuri, utilizate pentru a dezvolta o soluție, având ca punct de plecare un proiect detaliat, construit şi testat. Spiralele soluției în afara limitelor inițiale ale prototipului devin în mod progresiv mai scumpe şi mai detaliate. Analiza formală a riscurilor care trebuie să preceadă fiecare prototip şi prototipurile modificate, depinzând de iterațiile atinse, formează baza pentru dezvoltarea producției de produse software, incluzând specificarea cerințelor proiectului de sistem şi planurile testelor;
- **dezvoltarea activă** presupune divizarea sistemului în iterații relativ scurte, realizabile într-un timp limitat. Începând cu prima iterație, se urmăreşte obținerea funcționalității de lucru actuală, altfel existând posibilitatea ca software-ul realizat să nu coincidă cu pasul complet al unei iterații.

Dezvoltarea SI orientate pe date (*Data-Oriented System Development* - DOSD) este o metodă de reprezentare a cerințelor software concentrate pe date şi structura

acestora. Sunt instituții, cum ar fi bursele și servicii ale furnizorilor, liniile aeriene, companiile de telefoane etc., care generează date dependente de timp.

Aceste date sunt în formate precunoscute sau prespecificate, care pot fi pe un CD sau care pot fi descărcate prin protocoale FTP în fișiere cu extensii de tip CSV (*Comma Separated Value*) specifice anumitor tipuri de baze de date în care separatorul este virgula (programe cum sunt Excel sau Access utilizează acest format), ASCII specifice fișierelor de tip text, sau alte formate precizate. Utilizatorul organizației dezvoltă propria sa aplicație și poate folosi aceste date direct în aplicația sa, spre exemplu pentru a emite bilete de avion sau pentru a iniția cumpărarea sau vânzarea stocurilor către clienții săi. Avantajul major al abordării DOSD este că elimină erorile rezultate din transformarea datelor: cum ar fi transfer, conversie, transcriere și transpunere. Este în general combinată cu o altă tehnică de dezvoltare, care ia în considerare procesarea rezultatelor pentru a dezvolta o soluție proprie de afacere.

Dezvoltarea sistemelor orientate obiect (*Object-Oriented System Development* - OOSD) este procesul de specificare și de modelare a soluției, în care datele și procedurile sunt grupate într-o entitate numită obiect. Datele unui obiect sunt referite ca fiind atributele sale, iar funcțiile sale sunt referite ca metode. Aceasta este în opoziție cu abordarea structurată SDLC, care consideră datele separate de procedurile ce acționează asupra lor. Susținătorii OOSD consideră că asocierea între date și prelucrări reprezintă modul în care oamenii conceptualizează obiectele zi de zi. OOSD este o tehnică de programare și nu o metodologie de dezvoltare software în sine.

Obiectele sunt create pe baza claselor care sunt modele generale. Clasele reprezintă baza pentru cea mai mare parte a obiectelor proiectate. Ele pot fi de asemenea superclase (rădăcini sau clase-părinte), printr-un set de atribute de bază și metode sau subclase care moștenesc caracteristicile clasei-părinte și care, la cerere, pot adăuga sau înlătura funcționalități. În plus față de moștenire, clasele pot să interacționeze cu date folosite în comun, referindu-se la ele ca agregate sau componente grupate sau ca obiecte folosite în comun. Clasele agregate interacționează cu mesajele care sunt cereri de servicii ale unei clase, numită client, către o altă clasă, numită server. Abilitatea a două sau mai multe obiecte de a interpreta în mod diferit un mesaj în timpul execuției depinde de superclasa obiectului care apelează (polimorfism).

Pentru a realiza pe deplin beneficiile utilizării programării orientate pe obiect este necesar să fie abordate analiza și proiectarea orientată pe obiect. Lucrul cu obiectele permite analiștilor și programatorilor să considere aceste componente de logică ale sistemului și să clarifice în consecință procesul de programare.

Avantajele majore ale OOSD sunt următoarele:

- abilitatea de a conduce sau de a gestiona o mare varietate de tipuri de date;
- posibilitatea de reprezentare a unui complex de relații;
- capacitatea de a răspunde cererilor într-un mediu aflat în continuă schimbare.

Dezvoltarea bazată pe componente (*Component-Based Development*) poate fi privită ca dezvoltare a metodei orientate pe obiect. Ea presupune aplicaţii asamblate prin cooperarea unor pachete software care îşi pun la dispoziţie serviciile unor interfeţe definite (cum ar fi părţi de programe ajutătoare, numite obiecte, pentru a comunica cu altele, indiferent de limbajul de programare în care a fost scris sau sub care rulează sistemul de operare). **Componentele de bază sunt:**

- componente specifice în activitatea desfăşurată de client (*in-process client components*) se pot executa din interiorul unui process client, cum ar fi un browser;
- componente-client independente (*stand-alone client components*) – aplicaţii care îşi oferă serviciile altor aplicaţii software, putând fi utilizate drept componente în mod individual (de exemplu: EXCEL şi WORD din pachetul Microsoft);
- componente server independente (*stand-alone server components*) – procesele care rulează pe servere ce furnizează servicii standardizate pot fi la rândul lor aplicaţii. Acestea sunt iniţiate prin proceduri numite de comandă sau altele de acelaşi tip din cadrul unei reţele. Tehnologiile care suportă aceste aplicaţii includ componente de tip Microsoft (*Mirosoft's Distributed Component Object Model* - DCOM), *Object Management Group's Coommon Object Request Broker Architecture* (CORBA), *Sun's Java through Remonte Method Invocation* (RMI);
- componente într-un server de proces (*in-process server components*) – rulează pe servere în interiorul unor structuri numite containere. Exemple: *Micosoft's Tranzaction Server* (MTS) şi *Sun's Enterprise Java Beans* (EJB).

Avantajele utilizării componentelor în dezvoltarea SI:

- reduc timpul de dezvoltare prin utilizarea componentelor existente;
- îmbunătăţesc calitatea deoarece componentele existente au fost deja testate.
- permit concentrarea asupra funcţionalităţii afacerii şi mai puţin asupra programării;
- promovează modularitatea, încurajând sau forţând interfeţe puternice, între unităţi cu funcţionalitate distinctă;
- simplifică prin reutilizare deoarece componentele sunt în format executabil;
- reduc costurile de dezvoltare, deoarece costul componentelor software poate fi împărţit între mai mulţi utilizatori;
- susţin numeroase medii de dezvoltare. Componentele scrise într-un limbaj pot să interacţioneze cu componentele scrise în alte limbaje sau pot rula pe alte platforme;
- permit un compromis fericit între dezvoltarea unui SI sau achiziţionarea unuia existent. În schimbul cumpărării unei soluţii complete, care probabil nu răspunde întru totul cerinţelor, este posibil să se cumpere numai acele componente necesare care să fie încorporate ulterior, într-un sistem personalizat.

Luând în considerare aceste avantaje, trebuie acordată atenţie integrării software-ului dat nu numai în faza iniţială, dar şi în timpul procesului de dezvoltare. Nu are importanţă cât de eficientă este dezvoltarea componentei de bază, atâta timp cât cerinţele sistemului sunt incomplet definite, sau sistemul cade. Proiectul nu va avea succes.

Dezvoltarea aplicaţiilor web (*Web-based application development*)

Aplicaţiile web comparativ cu aplicaţiile locale au două caracteristici importante: accesul de la distanţă al utilizatorilor şi comunicarea între aplicaţii. Majoritatea dintre aceste aplicaţii sunt realizate în arhitectura client-server sau, mai nou, după modelul *web services*.

Principalele componente XML, utilizate pentru dezvoltarea aplicaţiilor web, sunt: SOAP (*Simple Object Access Protocol*), *Web Services Description Language* (WSDL) şi *Universal Description Discovery and Integration* (UDDI). Prima componentă SOAP se foloseşte pentru definirea interfeţelor de programare a aplicaţiei (*Application Programming Interface* - API) şi poate lucra cu orice limbaj de programare XML şi sub orice sistem de operare. Aceasta este uşor de utilizat şi are avantajul că realizează o cuplare slabă a modulelor, ceea ce permite ca o modificare într-un modul să nu necesite modificări şi în celelalte module.

A doua componentă WSDL permite descrierea serviciilor web care devin intrări şi ieşiri în modulele definite prin componenta SOAP. Aceasta poate fi utilizată şi pentru identificarea unui serviciu web accesibil prin intermediul unei reţele internet.

Componenta finală a serviciilor web – UDDI este utilizată pentru a realiza o intrare într-un director UDDI, care acţionează ca un director electronic accesibil din intranetul unei companii sau din cadrul internetului şi care permite părţilor interesate să înveţe despre existenţa serviciilor web disponibile.

Standardele pentru SOAP, WSDL şi UDDI au fost acceptate de consorţiul *World Wide Web* şi au fost create produse software şi medii de dezvoltare care suportă servicii web, inclusiv produsele *Microsoft Net*. Cu toate acestea, unele standarde importante, cum ar fi cel legat de securitate şi managementul tranzacţiilor, nu au fost încă definite.

Dezvoltarea aplicaţiilor web este diferită comparativ cu cea de a treia sau cea de a patra generaţie de programe din multe puncte de vedere, începând cu limbajele şi tehnicile de programare utilizate, continuând cu metodologiile (sau lipsa acestora) utilizate pentru a controla activitatea de dezvoltare, până la modalitatea în care utilizatorii testează şi acceptă aplicaţia.

Prototipizarea

Prototipizarea recunoscută ca o metodă euristică sau evolutivă de dezvoltare, reprezintă procesul de creare a unui SI, trecând de la încercările controlate şi erorile de procedură, la reducerea nivelului riscurilor în dezvoltarea sistemului. Aceasta înseamnă că permite dezvoltatorului şi clientului să înţeleagă şi să reacţioneze la riscurile fiecărui nivel de evoluţie, utilizând prototipizarea ca un mecanism de reducere a riscului. Prototipizarea combină cele mai bune trăsături ale clasicului SDCL prin menţinerea unei abordări sistematice, dar este încorporată într-un cadru de lucru iterativ, care reflectă lumea în mod real.

Cel mai adesea, prototipizarea reduce timpul de desfăşurare primară a sistemului prin utilizarea unor instrumente mai rapide de dezvoltare cum ar fi tehnica din generaţia a patra, care permite unui utilizator să aibă o privire de ansamblu asupra sistemului propus, într-o perioadă scurtă de timp.

Această metodă se bazează în faza de început pe prezentarea de rapoarte şi ecrane care sunt familiare utilizatorilor finali, permiţându-le acestora să înţeleagă modul de lucru al sistemului şi încurajându-i să participe la dezvoltarea SI. Există două metode de bază sau abordări de prototipizare:

1) Construirea modelului pentru a crea proiectul (mecanismul de definire a cerinţelor). Bazat pe acest model se va dezvolta proiectul sistemului cu toate trăsăturile necesare privind performanţa, calităţile şi întreţinerea acestuia;
2) În mod gradat, se va construi sistemul care urmează să fie pus în funcţie, utilizând limbajul de generaţie patru (4GL) care corespunde cel mai bine sistemului respectiv.

Prima abordare pune în evidenţă faptul că pot exista presiuni considerabile în implementarea prototipului iniţial. Adesea, utilizatorii, observând un model care lucrează, nu pot înţelege de ce prototipul iniţial trebuie ulterior rafinat. Realitatea este că prototipul trebuie ulterior extins pentru a face faţă volumului real de tranzacţii, conectivităţii în reţeaua client - server, crearea procedurilor de salvare şi recuperare, furnizarea datelor pentru control şi auditare.

Cea de a doua abordare lucrează în mod tipic cu aplicaţii mici, utilizând instrumente 4GL. Cu toate acestea, chiar dacă presupune un efort mai mare, este necesar să fie dezvoltat un proiect de strategie pentru sistem. Utilizând numai tehnicile 4GL, vor fi întâmpinate aceleaşi dificultăţi întâlnite în dezvoltarea aplicaţiilor de afaceri care utilizează abordări convenţionale (calitate slabă, întreţinere slabă, un grad scăzut de acceptare din partea utilizatorului).

Un alt dezavantaj al prototipizării este şi acela că, adesea, conduce spre funcţii sau părţi care ar trebui adăugate sistemului dar care nu au fost incluse în cerinţele

documentului inițial. Toate cerințele suplimentare față de cele ale documentului inițial trebuie să fie revizuite, pentru ca acestea să corespundă necesităților strategice ale organizației, având în vedere și costurile suplimentare pe care le-ar presupune. Altfel, sistemul final va funcționa **scump,** dar **ineficient**.

Un alt risc al sistemelor prototip este acela că sistemul final ar putea avea controale slabe. Concentrându-se în principal pe ceea ce solicită utilizatorul, dezvoltatorii de sistem ar putea neglija anumite controale, mai ales în cazul unei abordări tradiționale a dezvoltării, cum ar fi recuperări de date, securitate și probe de audit.

Schimbarea controlului aduce de multe ori complicații și mai mari sistemului prototip. Schimbările în proiectare și în cerințe pot fi uneori imprevizibile, existând riscul de a nu fi întotdeauna documentate și aprobate. În aceste cazuri sistemul poate să nu facă față și să ajungă în situația de a nu mai putea fi întreținut.

Cu toate că auditorul SI trebuie să fie conștient de riscurile asociate prototipizării, acesta trebuie să fie conștient și de faptul că această metodă de dezvoltare a sistemului poate fi furnizată organizației prin economisirea semnificativă de timp și costuri.

Dezvoltarea rapidă a aplicației (*Rapid Application Development* – RAD) este o metodologie care permite organizațiilor să dezvolte în mod strategic sisteme rapide, reducând în același timp costurile de realizare și menținând calitatea. Aceasta se obține utilizând o serie de tehnici de dezvoltare de aplicații despre care s-a demonstrat că au o metodologie bine definită. **Principalele elemente care permit utilizarea acestei metodologii:**

- echipe de dezvoltare mici, dar bine pregătite;
- prototipuri evolutive;
- integrarea de instrumente puternice care să suporte modelarea, prototipizarea și reutilizarea componentelor;
- cerințe interactive și ateliere de proiectare;
- timp limitat pentru dezvoltarea SI.

RAD susține analiza, proiectarea, dezvoltarea și implementarea unor aplicații informatice individuale, fără a defini necesarul de informații al unei organizații ca întreg sau al unei zone de afacere importantă din cadrul acesteia. RAD furnizează o direcție rapidă pentru dezvoltarea sistemului, concomitent cu reducerea costului și creșterea calității prin automatizarea unor părți importante ale SDLC, impunând linii rigide în dezvoltarea timpilor de construcție și reutilizare a componentelor existente.

Metodologia RAD are patru etape majore:

1) în etapa de definire a conceptului se specifică funcţiile afacerii şi sursa datelor de intrare, determinând în acelaşi timp şi scopul sistemului;
2) în etapa de proiectare funcţională se organizează ateliere de lucru pentru a modela datele sistemului şi procesele, pentru a construi un prototip de lucru al componentelor critice ale sistemului;
3) etapa dezvoltării completează construcţia bazei de date fizice şi a aplicaţiei-sistem, construieşte sistemul de conversie, dezvoltă elementele ajutătoare pentru utilizatori şi desfăşurarea planului de lucru;
4) etapa de distribuire include testarea finală de către utilizator, pregătirea conversiei de date şi implementarea SI.

RAD utilizează prototipizarea ca instrument central, indiferent sub ce tehnologie este utilizată.

Dezvoltarea activă (*agile development*)

Se referă la o familie de procese de dezvoltare similare care presupun o cale netradiţională de dezvoltare de sisteme complexe. O formă iniţială a dezvoltării active a apărut în anii '90, prin metoda de management de proiect SCRUM. Acesta are ca scop să transfere planificarea şi sarcinile directe de la managerul de proiect către echipă, părăsind munca managerului de proiect şi orientând obstacolele către echipă. De atunci au apărut următoarele procese active, cum ar fi: *Extreme Programming* (XP), *Crystal*, *Adaptive Software Development*, *Feature Driven Development* şi *Dynamic Systemens Development Method*. Aceste procese se numesc active pentru că sunt proiectate să facă faţă în mod flexibil schimbărilor dezvoltării sistemului sau proiectului care reprezintă rezultatul dezvoltării.

Reingineria (*reengineering*) este un proces de a actualizare a unui sistem existent extrăgând şi reutilizând proiectul şi componentele programului. Acest proces este utilizat pentru a suporta schimbări majore în modul de operare al organizaţiei.

Ingineria inversă (*reverse engineering*) este un proces de descompunere a unei aplicaţii, a unui software de aplicaţie sau a unui produs, pentru a vedea cum funcţionează fiecare în parte, utilizând această informaţie pentru a dezvolta un sistem similar. Acest proces poate avea loc prin mai multe modalităţi:

- decompilarea programelor-obiect sau executabile în programe-sursă care vor permite apoi analiza acestora;
- utilizând aplicaţia de inginerie inversă ca un test de cutie neagră şi dezvăluind funcţionalitatea sa prin utilizarea unor date de test.

Avantajele majore ale ingineriei inverse sunt:

- dezvoltarea rapidă şi reducerea duratei SDLC;
- crearea unui sistem îmbunătăţit, utilizând schiţele aplicaţiei reversului ingineriei.

Auditorul SI trebuie să aibă în vedere următoarele riscuri:

- acordul privind licența software conține adesea clauze prohibitive ale licenței software-ului ingineriei inverse, astfel încât orice înțelegere secretă sau tehnici de programare să nu fie compromise;
- decompilările dispun de instrumente relativ noi cu funcții care depind de calculatoare specifice, sisteme de operare și limbaje de programare. Orice schimbare într-una dintre aceste componente solicită dezvoltarea sau achiziționarea unui nou decompilator.

3.3.4. Reingineria proceselor de afaceri (*Business Process Reengineering* - BPR)

„O afacere reprezintă în esență înțelegerea proceselor aflate în componența ei și succesul unei afaceri implică o înlănțuire eficientă a proceselor componente. Orice alte elemente constitutive ale unei afaceri își pierd unicitatea devenind simple pârghii ale acesteia. Acesta este motivul pentru care organizarea eficientă a proceselor devine principalul punct pe agenda managementului oriunde în lume."[4]

Un proces de afaceri poate fi privit ca fiind un sistem sociotehnic, ceea ce înseamnă că reprezintă „un set de activități de muncă interrelaționată, caracterizat prin intrări specifice și cerințe care aduc plusvaloare, generând ieșiri specifice axate pe nevoile consumatorilor. Procesul afacerii constă în fluxuri de muncă orizontale ce străbat numeroase departamente."[5]

Reingineria proceselor de afaceri reprezintă o etapă în cadrul căreia trebuie să existe răspuns la presiunile competitivității, economiei și dorințelor consumatorilor, în scopul supraviețuirii într-un mediu specific afacerilor. Acest lucru se realizează de obicei prin automatizarea proceselor de sistem în scopul diminuării numărului de intervenții și controale efectuate manual. Reingineria proceselor de afaceri obținută cu ajutorul implementării unui sistem de planificare a resurselor companiei (*Enterprise Resources Planning* - ERP) se referă deseori la un pachet care facilitează reingineria (*Package-Enabled Reengineering* - PER). Avantajele reingineriei proceselor de afaceri sunt deseori întâlnite acolo unde aceasta se pliază perfect la nevoile afacerii.

În reingineria proceselor de afaceri preocuparea principală a auditorului sistemului informatic se referă la identificarea controalelor-cheie existente și evaluarea impactului înlocuirii acestora. În cazul controalelor-cheie de prevenire, auditorul SI trebuie să se asigure că managementul este conștient de schimbarea controalelor respective și că acesta este dispus să accepte riscul material potențial generat de lipsa acestor controale.

[4] N.S. Nagaraj et al., *BPM Part I: An Emerging Trend*, SETLabs, 2001.

[5] Sethi/King, *Introduction to BPR*, p.4.

Procesul de benchmarking este definit ca fiind un proces continuu şi sistematic, cu ajutorul căruia sunt evaluate produsele, serviciile şi procesele de muncă ale organizaţiei, recunoscut a fi o practică eficientă pentru îmbunătăţirea organizaţiei.

Acest proces presupune parcurgerea următoarelor etape:

1. **planificarea** - echipa de *benchmarking* trebuie să identifice procesele critice şi să înţeleagă modul în care acestea sunt măsurate, tipul de date necesare şi modul în care acestea trebuie colectate;
2. **cercetarea** - echipa trebuie să colecteze date de bază despre propriul proces, înainte de a colecta date despre alţii. Următoarea etapă se referă la identificarea partenerilor de *benchmarking* prin surse precum ziarele şi revistele de afaceri, deţinătorii premiilor de calitate, jurnalele de afaceri etc;
3. **observarea** constă în colectarea datelor şi vizitarea partenerilor de *benchmarking*. Pentru aceasta, ar trebui să existe o înţelegere încheiată cu o organizaţie parteneră, un plan de colectare a datelor şi o modalitate de facilitare a propriei observări;
4. **analiza** implică gruparea şi interpretarea datelor colectate şi analizarea diferenţelor dintre procesul organizaţiei luate în calcul şi cel al unei organizaţii partenere. Convertirea elementelor-cheie descoperite prin compararea celor două procese în noile scopuri operaţionale va deveni ţelul acestei etape;
5. **adaptarea** rezultatelor de benchmarking este considerată a fi etapa cea mai dificilă. În cadrul acesteia, echipa are nevoie să transforme constatările în principii-cheie şi să le transpună mai departe în strategii şi apoi în planuri de acţiune;
6. **îmbunătăţirea continuă** reprezintă de fapt elementul-cheie al exerciţiului de *benchmarking,* care trebuie să coreleze strategia de îmbunătăţire cu scopurile acesteia.

Auditul şi evaluarea tehnicilor reingineriei procesului afacerii – în momentul în care sunt revizuite eforturile schimbării procesului de afaceri al unei organizaţii, auditorii SI trebuie să determine dacă:

- eforturile schimbării organizaţiei sunt în concordanţă cu cultura şi cu planul strategic al acesteia;
- echipa de reinginerie face eforturi în scopul minimizării oricărui impact negativ pe care schimbarea l-ar putea avea asupra personalului organizaţiei;
- echipa de management a schimbării a asimilat o serie de lecţii documentate în urma reingineriei procesului afacerii.

În privinţa fiabilităţii SI există **standardul ISO 9126** care defineşte fiabilitatea ca un set de atribute bazat pe capabilitatea SI de a-şi menţine nivelul de performanţă, în condiţii şi pe o perioadă de timp stabilite. Analiza acestei caracteristici pune accentul

toleranța la defecte și corectitudine. Tehnicile de obținere a toleranței la defecte se aplică în special la componentele hardware și la sisteme de operare. Principala problemă în programare este corectitudinea sistemelor de programe, în sensul că acestea trebuie să îndeplinească specificațiile funcționale stabilite.

- **funcționalitatea** *(functionality)* - calitatea software-ului poate fi definită de următoarele atribute bazate pe existența unui set de funcții și pe proprietățile lor specificate, care satisfac necesitățile stabilite sau implicite;
- **siguranța în utilizare** *(reliability)* este o caracteristică ce stabilește măsura în care un sistem de programe nu permite efectuarea de modificări neautorizate, menținându-se nivelul de performanță stabilit în condiții bine determinate;
- **utilizabilitatea** *(usability)* este definită ca un set de atribute bazate pe efortul necesar pentru utilizarea produsului software și pe evaluarea individuală a utilizării acestuia, de către un grup stabilit sau implicit de utilizatori;
- **eficiența** *(effciency)* este definită ca un set de atribute bazat pe relația dintre nivelul de performanță a produsului software și cantitatea de resurse utilizate, în anumite condiții stabilite;
- **mentenabilitatea** *(maintainability)* este definită ca un set de atribute bazate pe efortul necesar de a face modificările specificate în produsul software respectiv. Acestea includ corecții, îmbunătățiri sau adaptări la modificări ale platformelor de dezvoltare sau ale celor cărora le sunt destinate, modificări în cerințe și specificații funcționale. Se poate spune că un produs software este mentenabil în măsura în care permite o actualizare rapidă și ușoară, astfel încât să se utilizeze în continuare, în bune condiții. Nivelul mentenabilității se stabilește pe baza datelor obținute în etapele de proiectare, testare și utilizare curentă;
- **portabilitatea** *(portability)* este definită ca o caracteristică de ordin calitativ a sistemelor de programe ce pot fi executate pe mai multe tipuri de calculatoare. Asigurarea portabilității sistemelor de programe contribuie la menținerea fiabilității la nivel ridicat.

Modelul de maturitate a capacităților software-ului (*Software Capability Maturity Model* - CMM), dezvoltat de Institutul de Inginerie Software al Universității Carnegi Melon, este un set de reguli care sprijină organizațiile în îmbunătățirea proceselor ciclului de viață al software-ului lor. Modelul permite organizațiilor să prevină întârzieri excesive în planificarea proiectului sau depășirea costurilor, prin furnizarea unei infrastructuri potrivite și a unui suport necesar, ajutând proiectele să evite aceste probleme.

Bazat pe principalele cinci niveluri ale procesului de management al calității, CMM a fost proiectat să ghideze organizațiile software în selectarea strategiilor de îmbunătățire a procesului prin determinarea maturității procesului și prin identificarea câtorva puncte critice în scopul îmbunătățirii calității software-ului. Aceasta permite organizațiilor să se concentreze asupra unui set limitat de activități pentru a

îmbunătăţi procesul software. **Cele cinci niveluri de maturitate care pot fi atinse de software-ul organizaţiilor sunt:**

1. **iniţial** – caracterizat ca un nivel *ad hoc*, în care succesul depinde doar de efortul individual;
2. **repetabilitatea** – buna organizare a proceselor de management prin care sunt stabilite planificarea şi urmărirea costului, programarea şi funcţionalitatea, care oferă o privire de ansamblu asupra proiectului software. Acestea creează un mediu de învăţare în care procesele definite şi aplicate cu succes pot fi repetate cu succes asupra altor proiecte de dimensiuni similare şi cu un scop asemănător;
3. **definirea** – lecţiile învăţate din fazele anterioare furnizează determinarea pentru dezvoltarea unui proces software standard în cadrul organizaţiei. Acesta include atât activităţile de management, cât şi cele de inginerie software, documentare, standardizare şi integrare într-un proces software instituţionalizat, aplicabil tuturor proiectelor de dezvoltare software;
4. **conducerea** – odată ce un proces este bine definit şi aplicat, organizaţia a atins punctul din care ea poate dezvolta şi aplica măsura controlului conducerii privind procesele dezvoltării software-ului. Acesta furnizează un grad mare de precizie şi control asupra proiectelor software pentru îmbunătăţirea productivităţii software şi atingerea obiectivului de a nu avea defecte (*zero-defect goals*);
5. **optimizarea** – când o organizaţie a dobândit abilitatea de a controla cantitativ şi cu succes proiectele software, se află într-o poziţie optimă de a utiliza strategii de îmbunătăţire continuă a procesului în scopul aplicării soluţiilor novatoare şi a tehnologiilor performante (*state-of-the-art*) propriilor procese software.

Îmbunătăţirea activităţilor dezvoltate de o organizaţie apare între nivelurile de maturitate doi şi cinci. Punctul de pornire este acela al unui nivel deasupra nivelului de maturitate actual al organizaţiei.

3.4. Controalele aplicaţiilor

3.4.1. Necesitatea controalelor aplicaţiilor

Controalele aplicaţiilor sunt specifice fiecărei aplicaţii şi au rolul de a asigura completitudinea şi acurateţea înregistrărilor şi prelucrărilor. Controalele sunt manuale sau automate şi se aplică intrărilor, prelucrărilor şi ieşirilor aplicaţiilor.

Înainte de a proceda la prezentarea controalelor aplicaţiilor considerăm necesar a preciza necesitatea înţelegerii interdependenţei dintre controlale generale şi controalele aplicaţiilor. Introducerea unui nou sistem poate determina deficienţe la nivelul controalelor generale care, la rândul lor, vor afecta în sens negativ

funcționarea eficientă a controalelor aplicațiilor. Chiar dacă controalele aplicațiilor vor continua să funcționeze, dacă controalele generale sunt inadecvate, riscul ca acestea (controalele aplicațiilor) să fie îngrădite este ridicat. Controlele generale sunt necesare ca suport în funcționarea controalelor aplicațiilor, dar ambele sunt necesare pentru a asigura procesarea completă și corectă a informațiilor.

Controalele aplicațiilor trebuie să asigure faptul că:

- sunt introduse în aplicații doar date valide, complete și corecte, asigurându-se integritatea și credibilitatea acestora;
- procesarea datelor se desfășoară corect, iar datele din sistem sunt corecte, relevante, protejate împotriva accesului neautorizat și disponibile la nevoie;
- ieșirile prelucrărilor sunt corecte, răspunzând specificațiilor;
- se asigură actualizarea datelor.

Controalele aplicațiilor sunt reprezentate de: teste de editare, totaluri, reconcilieri etc., care vor permite identificarea și raportarea datelor incorecte, lipsă și excepțiile. Investigarea corectă a excepțiilor presupune derularea atât de controale automate, cât și de proceduri manuale.

Consistența, acuratețea și continuitatea controalelor din sistem oferă auditorului certitudinea asupra acurateței și completitudinii datelor, calității prelucrărilor ceea ce îl va ajuta la determinarea naturii, întinderii și complexității testelor pe care urmează să le desfășoare. Complexitatea sistemelor informatice de gestiune impune necesitatea abordării lor pe subsisteme și o solidă documentare a auditorului cu privire la sistemul auditat. Auditorul trebuie să identifice și să cunoască orice documentație a aplicației existentă la client sau să valorifice orice sursă de documentare care-i poate furniza informații suplimentare. În vederea realizării sarcinilor sale, auditorul sistemului informațional trebuie să:

- identifice componentele semnificative ale aplicației;
- înțeleagă fluxul tranzacțiilor. În acest sens el poate apela la realizarea de diagrame ale fluxurilor de date pentru evidențierea: intrărilor, fișierelor utilizate, procesărilor, ieșirilor, controalelor manuale și automate implementate, evaluând măsura în care sunt suficiente și acoperitoare;
- testeze controalele pentru a avea certitudinea că acestea funcționează corect și eficient. Auditorul va trebui să răspundă la următoarele întrebări:
    - Care sunt controalele de bază?
    - Se suprapun, în unele cazuri, controalele manuale peste cele automate? Acest lucru crește gradul de încredere asupra controalelor?
    - Care sunt controalele interdependente din cadrul aplicației?
    - Cine are responsabilitatea acestor controale?

- evaluarea adecvării şi eficienţei controalelor, evidenţiind punctele forte şi slabe ale acestora şi consecinţele ineficienţei şi inadecvării acestora. Pentru aceasta se procedează la valorificarea rezultatelor testelor efectuate;
- compararea aspectelor operaţionale ale aplicaţiei cu standardele de programare.

3.4.2. Controlul intrărilor

Este folosit pentru a se asigura faptul că toate datele sunt introduse corect, complete, valide, autorizate, aferente perioadei de gestiune curente, înregistrate corect în conturi (în cazul aplicaţiilor contabile).

În egală măsură trebuie să subliniem faptul că în cadrul mediilor de procesare integrată ieşirile unui sistem devin intrări pentru un altul. De aceea auditorul trebuie să cunoască sistemul informatic în toată complexitatea sa şi să înţeleagă corect fluxul tranzacţiilor.

Autorizarea

Autorizarea intrărilor reduce riscul erorilor, fraudei şi tranzacţiilor ilegale. Autorizarea poate fi controlată prin identificarea utilizatorului, care a introdus datele în sistem, pe baza privilegiilor asociate ID-urilor utilizatorilor. Auditorul va trebui să verifice dacă se introduc doar date autorizate în sistem, cine şi cum autorizează datele de intrare.

Autorizarea se poate efectua on-line la momentul introducerii datelor. Principiul segregării atribuţiilor determină efectuarea a doi paşi distincţi de către doi utilizatori autorizaţi să aibă acces la aplicaţie: introducerea datelor şi respectiv autorizarea datelor. Este deosebit de importantă existenţa unor controale care să asigure că datele autorizate rămân neschimbate.

În cadrul aplicaţiilor pot fi identificate mai multe tipuri de autorizări:

- *semnarea documentelor* primare sau a formularelor de tip batch;
- *controale ale accesului* asigurând ca doar persoanele autorizate să poată avea acces la aplicaţie pentru introducerea de date şi respectiv executarea procesărilor;
- *parole unice* asigurând mijloace sigure de identificare a accesului autorizat;
- *identificarea staţiilor de lucru sau terminalelor:* permite limitarea introducerilor de date la anumite staţii de lucru/terminale, dar şi a utilizatorilor (restricţionaţi să lucreze pe anume terminale/staţii);

- *documente-sursă*: un document-sursă poate fi un document pe suport hârtie sau un formular afişat on-line. Proiectarea corectă a documentelor asigură viteză la introducerea datelor, dar ceea ce este şi mai important limitează riscul de eroare a datelor introduse, controlează fluxul datelor, sporeşte viteza şi acuratețea cu care datele pot fi citite. Aceste documente-sursă sunt pretipărite şi se caracterizează prin:
  - gruparea câmpurilor similare pentru facilitatea introducerii de date;
  - oferă coduri predefinite pentru introducerea datelor care să permită limitarea erorilor;
  - conțin identificatori utili în căutarea şi urmărirea tranzacțiilor;
  - asigură spații rezervate autorizării de către management.

Validarea intrărilor se poate realiza manual sau automat şi reduce riscul introducerii de date incorecte.

Maxima *garbage in – garbage out* atenționează asupra importanței acurateței datelor de intrare. Este mai eficient să aloci resurse pentru asigurarea acurateței şi completitudinii datelor de intrare decât să fii nevoit să le corectezi în timpul sau, mai grav, după încheierea procesului de prelucrare şi chiar a depunerii rapoartelor.

Controlul datelor de intrare trebuie adaptat la modalitățile diferite de introducere a datelor în sistem:
- de la tastatură (unde riscul erorilor este mai mare);
- scanarea documentelor;
- utilizarea perifericelor senzoriale;
- citirea barelor de cod;
- ATM-uri şi terminale POS;
- EDI (*Electronic Data Interchange*);
- generarea automată a tranzacțiilor (exemplu: plăți planificate, calcularea lunară a dobânzilor).

O particularitate a aplicațiilor de gestiune constă în faptul că nu toate intrările prezintă un suport material (documente pe suport hârtie), multe fiind în format electronic. În cazul preluării automate sau generării automate există riscuri mai mici de eroare față de preluarea datelor prin tastare.

Tipuri de controale aplicate asupra datelor de intrare
Controale specifice introducerii de tranzacții pe loturi

Controale specifice introducerii de date pe loturi asigură controlul la nivelul totalurilor calculate pentru lotul respectiv de documente. Literatura de specialitate recomandă utilizarea următoarelor tipuri de astfel de controale:

- **totalul întregistrărilor** (*total items*): verificarea faptului că totalul poziţiilor din documentele justificative aparţinând unui lot de documente este egal cu totalul înregistrărilor introduse. Spre exemplificare, să presupunem că un lot de facturi urmează a fi introdus în aplicaţia de gestiune. Fiecare factură prezintă un număr de poziţii corespunzătoare produselor facturate. Controlul prin totalul numărului de întregistrări evidenţiază dacă au fost introduse toate poziţiile înscrise în lotul de facturi ce trebuia procesat.

- **totalul valorilor monetare** (*total monetary amount*) presupune verificarea egalităţii între totalul unui câmp monetar dintr-o înregistrare determinat în mod automat şi totalul aceluiaşi câmp calculat independent pe baza documentelor existente în lot. În cazul identităţii celor două totaluri înseamnă că toate documentele au fost introduse corect. Revenind la exemplu de mai sus, acest control al valorilor monetare se poate aplica câmpului valoare produs aferent fiecărei poziţii din facturile lotului.

- **totalul documentelor** (*total documents*) presupune verificarea egalităţii între totalul numărului de documente procesate (existente în lot) şi totalul documentelor introduse prin intermediul aplicaţiei şi determinat automat de aceasta.

- **totalurile aplicate câmpurilor numerice predeterminate** (*hash totals*) presupun verificarea egalităţii între totalul obţinut prin însumarea valorii câmpului predeterminat pentru tot lotul de documente şi valoarea calculată prin sistem pentru acelaşi câmp. Revenind la exemplul cu lotul de facturi, în cazul unei aplicaţii de contabilitate acest total poate fi aplicat simbolului contului de furnizor. Pentru un lot de zece facturi totalul ar fi 4010 (10×401, unde 401 este simbolul contului de furnizori). Acest total arată dacă s-au introdus toate facturile şi/sau toate simbolurile de conturi s-au introdus corect (întotdeauna 401).

În cazul introducerii documentelor pe loturi este bine să fie utilizate documente pretipărite, prezentând valori pretipărite pentru toate câmpurile care se pretează la o astfel de atribuire de valori scopul urmărit fiind limitarea erorilor la introducerea datelor (ex. Codul tranzacţiei, număr factură - pentru cele emise de firmă etc).

Raportarea şi corectarea erorilor

Aplicaţiile trebuie să dispună de controalele necesare validării datelor şi identificării tranzacţiilor duplicate. Aceste erori de introducere a datelor pot afecta semnificativ completitudinea şi acurateţea datelor. De aceea se procedează la:

- respingerea tranzacţiilor eronate care nu au trecut de controalele de validare, restul tranzacţiilor fiind procesate;
- respingerea întregului lot de tranzacţii;
- ţinerea lotului în aşteptare până la corectarea erorilor;
- acceptarea lotului şi marcarea tranzacţiilor conţinând erori pentru efectuarea ulterioară a corecţiilor.

Tehnicile de control al intrărilor sunt:

- **jurnalul tranzacțiilor** (*transaction log*) conține lista detaliată a tuturor actualizărilor. Jurnalul poate fi realizat manual sau automat. În practică se procedează la reconcilierea între numărul de documente introduse și numătul tranzacțiilor înscrise în jurnal;
- **reconcilierea datelor** permite verificarea faptului că toate datele primite au fost înregistrate corect și procesate;
- **documentația** se referă la evidența scrisă realizată de utilizator cu privire la datele introduse (număr de documente) și rezultatele procedurilor de control;
- **procedurile de corectare a erorilor** includ:
  1. înregistrarea erorilor;
  2. efectuarea corecțiilor la timp;
  3. aprobarea corecțiilor;
  4. suspendarea fișierului;
  5. crearea fișierului de erori;
  6. validarea corecțiilor.
- **anticiparea**: utilizatorul sau controlul de grup anticipează primirea datelor;
- **jurnalul transmiterilor** (*transmital log*). Documentele de transmitere sau primire a datelor;
- **anularea documentelor-sursă**: marcarea documentelor care au fost introduse pentru a se evita introducerea duplicată.

Controlul integrității loturilor se aplică și în cazul sistemelor online sau a bazelor de date. Loturile pot fi stabilite în acest caz la nivelul tranzacțiilor unei zile, tranzacțiilor introduse de la un anume terminal sau de o anumită persoană.

3.4.3. Proceduri de prelucrare și control

Auditorul sistemului informatic trebuie să cunoască și să înțeleagă procedurile și controalele care se execută în cadrul acestora pentru a evalua măsura în care aceste controale sunt adecvate, suficiente și eficiente.

Validarea datelor și proceduri de editare

Aplicațiile trebuie să asigure faptul că datele introduse sunt validate și editate cât mai aproape de momentul inițierii operației de introducere. Utilizarea formatelor predefinite pentru introducerea datelor asigură introducerea corectă a datelor în câmpuri și respectarea formatului predefinit al câmpurilor. Dacă procedurile de introducere a datelor permit supervizorilor să „ocolească” validarea datelor și editarea, atunci este necesară generarea automată de jurnale ale tranzacțiilor.

Validarea datelor permite identificarea erorilor, incompletitudinii, inconsistenţei sau a lipsei datelor. Editarea şi validarea *front-end* a datelor se poate realiza şi prin intermediul unor terminale inteligente.

Controalele de editare sunt controale preventive deoarece ele nu permit procesarea de date eronate. Dacă aceste controale nu sunt eficiente este afectat procesul de prelucrare prin procesarea de date inexacte. Aplicaţiile pot cuprinde următoarele tipuri de controale de validare şi editare:

A. Controlul formatului

Se verifică:

- natura datelor;
- lungimea datelor (evitarea producerii de trunchieri);
- numărul de zecimale admis;
- acceptarea valorilor negative sau doar a celor pozitive;
- formatul datei calendaristice;
- aplicarea semnului monetar.

B. Controlul domeniului de definiţie a atributelor

Urmăreşte:

- încadrarea într-o mulţime de valori prestabilită (*validity check*). Exemplu: abrevierile judeţelor, tipuri de unităţi de măsură, tipuri de documente;

- încadrarea într-un interval de valori prestabilit (*range check*). Exemplu: salariul angajaţilor ia valori în intervalul [3.500, 30.000];

- respectarea unei valori limită (*limit check*). Exemplu: un câmp nu poate lua valori peste o anumită limită (bursa unui student nu poate depăşi 400 RON);

- respectarea secvenţei de valori atribuite unui câmp (*sequence check*). Exemplu: numărul facturii emise de firmă trebuie să respecte secvenţa numerelor aferente facturierului;

- validările realizărilor unor atribute diferite, numit şi testul dependenţei logice dintre câmpuri (*logical relationship check*). Exemplu: validările privind corespondenţa conturilor – contul X se poate debita doar prin creditarea conturilor A, B sau C;

- testul „rezonabilităţii" datelor (*reasonableness check*): Acest test verifică dacă datele sunt rezonabile în raport cu un standard sau date introduse în perioade anterioare. Datele standard pot fi stocate într-un fişier sau pot reprezenta

constante definite la nivelul aplicaţiei (exemplu: un standard poate fi reprezentat de numărul de ore lucrătoare într-o lună stabilit în funcţie de zilele lucrătoare şi sărbătorile legale, nivelurile de dobândă practicate de bancă etc.);

- respectarea valorilor specificate în cadrul unor grile, tabele (*table look-ups*). Testul verifică măsura în care datele introduse respectă criterii predefinite stabilite prin tabele de valori reţinute în aplicaţie. Spre exemplu în cazul sporurilor de vechime aplicaţia va reţine sporul aferent fiecărui interval de vechime stabilit prin reglementările în domeniu;
- testul completitudinii (*completness check*): câmpul trebuie să cuprindă orice alt caracter decât zero sau spaţiu. Verificarea se realizează pentru fiecare digit din componenţa câmpului.

C. Controlul acurateţei aritmetice

Pe baza unor date de intrare introduse de operator pot fi verificate elementele calculate din documentul primar. De exemplu, pe baza cantităţii şi a preţului unitar al unui articol înscris într-o factură, sistemul generează automat pe ecran valoarea produsului, a TVA, valoarea cu TVA şi apoi totalul facturii, operatorul putând confrunta aceste sume calculate cu cele înscrise în factură.

D. Controlul existenţei datelor (existence check)

Testul se referă în principal la validarea datelor de intrare reprezentând coduri. Este suficient să introduci codul unul client şi pe ecran să se afişeze numele acestuia sau un mesaj de eroare atenţionând asupra introducerii unui cod incorect/inexistent.

E. Testul cifrei de control (check digit)

Se aplică asupra datelor de intrare reprezentând elemente codificate şi urmăreşte respingerea codurilor eronat introduse. Cauza erorii la nivelul elementelor codificate poate fi:

- trunchierea;
- adăugarea unui caracter suplimentar;
- transcrierea incorectă a codului în documentul primar;
- transpoziţia caracterelor la introducerea codului.

Testul cifrei de control presupune determinarea cifrei de control aferente codului introdus prin aplicarea automată a algoritmului prestabilit. În măsura în care cifra de control determinată automat nu corespunde celei incluse în codul introdus de operator sistemul va trebui să atenţioneze printr-un mesaj corespunzător asupra erorii apărute şi să nu permită salvarea datelor introduse.

F. Testul tranzacţiilor duplicate (duplicate check)

Auditorul va trebui să verifice dacă sistemul admite introducerea repetată a aceloraşi date. De exemplu, introducerea repetată a unui aceluiaşi document (factură, bon de consum etc).

Soluţionarea tranzacţiilor respinse

Auditorul va trebui să verifice:

- cum se soluţionează tranzacţiile neacceptate de sistem (care nu au trecut testul de validare);
- cine răspunde de verificarea acestor date de intrare şi de reintroducerea lor;
- dacă sunt generate liste conţinând intrările respinse.

Dacă aceste tranzacţii respinse sunt consemnate în documentele primare, depistarea erorii este mai uşoară şi corectarea se poate face fără probleme deosebite. Probleme particulare apar în cazul tranzacţiilor on-line.

Controalele prelucrării datelor

Controalele de procesare asigură completitudinea şi acurateţea datelor şi posibilitatea efectuării doar de modificări autorizate. Tehnicile de asigurare a acurateţei şi completitudinii datelor sunt:

1. **recalculări manuale**: pentru un eşantion de date se procedează la recalculări manuale pentru a se verifica dacă s-au realizat corect prelucrările prevăzute prin aplicaţie;
2. **editare**: un control de editare se realizează printr-un program sau subrutină care pemite verificarea acurateţei, completitudinii şi validităţii datelor. Un astfel de program poate fi utilizat în verificarea datelor introduse sau după procesarea datelor;
3. **verificări de-a lungul stadiilor de prelucrare** (*run-to-run totals*) oferă posibilitatea de a verifica valorile datelor în diferitele stadii de prelucrare. Exemplu: numărul înregistrărilor citite este egal cu cel al înregistrărilor actualizate;
4. **controale programate** (*programmed controls*): programele trebuie să identifice şi să corecteze erorile în procesarea datelor. Spre exemplu, în cazul procesării unui fişier sau a unei versiuni incorecte se va emite un mesaj de atenţionare;
5. **rezonabilitatea valorilor calculate** (*reasonableness verification of calculated amounts*): aplicaţiile pot conţine controale pentru verificarea rezonabilităţii valorilor calculate în raport cu unele criterii prestabilite. Tranzacţiile care nu trec acest test vor fi respinse şi supuse unei verificări.
6. **valori limită pentru câmpuri calculate** (*limit ckecks on calculated amounts*): valorile calculate sunt verificate în raport cu valori limită

prestabilite. Tranzacțiile care nu trec acest test vor fi respinse și supuse unei verificări;

7. **reconcilierea totalurilor fișierului** (*reconciliation of file totals*): reconcilierea se poate realiza în raport cu totaluri realizate manual, cu un fișier de control independent sau controlul înregistrărilor fișierului;
8. **lista înregistrărilor eronate** (*exception report*): se procedează la listarea înregistrărilor care nu au trecut de controalele de validare.

Proceduri de control al fișierelor

Controalele asupra fișierelor urmăresc ca doar prelucrările autorizate să fie executate asupra datelor stocate. Fișierele supuse acestor controale sunt reprezentate de:

- parametrii de control ai sistemului (*system control parameters*): importanța controlului acestor intrări este dată de faptul că acești parametri pot schimba modul de lucru al sistemului și afecta controalele realizate de sistem. De aceea orice modificări în aceste fișiere trebuie controlate și autorizate la fel ca în cazul modificărilor de programe;
- constante (*standing data*) reprezintă date care nu cunosc modificări frecvente în timp (simboluri de conturi, codul de identificare al angajaților, codul și adresa furnizorilor și clienților etc.). De aceea orice modificări în aceste fișiere trebuie aprobate și înregistrate ca probe de audit;
- fișierele master/balanțe (*Master data/balance data*) - executarea balanțelor și totalurilor actualizate în baza tranzacțiilor nu pot fi ajustate decât sub un control strict și aprobat. Procesele de audit trail sunt importante în acest caz deoarece rapoartele pot avea implicații asupra datelor financiare ale firmei;
- fișiere de tranzacții (*transaction files*) sunt supuse controlului prin validări, controale ale totalurilor, limitele înregistrărilor respinse etc.

Prezentăm câteva dintre controalele asupra fișierelor:

1. raportarea erorilor de întreținere și manipulare (*maintenance errors reporting and handling*): controalele procedurilor trebuie să ofere siguranța că toate erorile raportate au fost reconciliate la timp și corectate. Principiul segregării funcțiilor incompatibile impune ca persoana care soluționează erorile să fie diferită de cea care a introdus datele în sistem;
2. reținerea documentelor-sursă (*source documentation retention*): documentele-sursă trebuie păstrate pe o perioadă de timp adecvată în raport cu natura informațiilor conținute (pentru unele dintre aceste documente există prevederi legale privind perioada de păstrare). Pe baza documentelor-sursă se poate proceda la regăsirea, reconstituirea și/sau verificarea datelor. De aceea este necesară elaborarea unei politici privind păstrarea documentelor și a procedurilor de distrugere a acestora după ce perioada de păstrare a expirat;

3. etichetarea internă şi externă (*internal and external labeling*): modul de etichetare a volumelor de memorie externă este extrem de important pentru identificarea şi procesarea corectă a datelor stocate în acestea. Etichetarea internă este utilă verificărilor automate privind corectitudinea fişierelor supuse prelurării;
4. versiunea fişierelor (*version usage*) este necesară verificarea versiunii fişierului supus prelucrării pentru a avea certitudinea că este cea corectă;
5. securitatea fişierelor (*data file security*): controalele securităţii fişierului nu privesc acurateţea datelor, ci dau siguranţa că nu a fost permis accesul persoanelor neautorizate la aplicaţie pentru a se modifica datele stocate;
6. reconcilierea listelor cu tranzacţii cu documentele sursă (*one-to-one checking*): pentru a avea certitudinea că s-au introdus corect toate documentele se procedează la verificarea jurnalului înregistrărilor cu fiecare document primar;
7. intrări preînregistrate (*prerecorded input*): anumite câmpuri prezinţă valori implicite în ecranele de introducere date pentru a se diminua riscul erorii de culegere a datelor de la tastatură;
8. jurnalele tranzacţiilor (*transaction logs*): se procedează la listarea tranzacţiilor introduse de fiecare operator (jurnalul va cuprinde informaţia privind ID-ul persoanei care a introdus datele şi staţia de la care a lucrat);
9. autorizarea actualizării şi întreţinerii fişierelor (*file updating and maintenance authorization*): trebuie să existe autorizarea actualizărilor efectuate pentru a avea certitudinea că datele sunt protejate în mod adecvat. Aplicaţiile trebuie să cuprindă controale privind restricţiile de acces;
10. verificarea de paritate (*parity check*) reprezintă o tehnică de control asupra datelor transmise prin căile de comunicaţie. Transmisiile se verifică prin tehnici de detectare a erorilor de tipul verificării prin lungimea măsurată în biţi a datelor transmise sau identificarea transmisiilor redundante.

Controlul fişierelor reprezintă o activitate laborioasă şi deosebit de importantă în procesul auditării aplicaţiei. Acest lucru este urmarea faptului că realitatea şi corectitudinea informaţiilor generate de aplicaţia auditată sunt determinate în egală măsură de acurateţea datelor prelucrate, precum şi de acurateţea prelucrărilor. De aceea auditorul va trebui să verifice şi următoarele aspecte:

- continuitatea fişierelor;
- modul de migrare a datelor de pe o aplicaţie pe alta. Se verifică măsura în care:
  - au fost autorizate procedurile de transfer al fişierelor din vechea în noua aplicaţie;
  - procedurile au fost realizate de persoanele împuternicite;
  - s-a asigurat completitudinea şi corectitudinea transferului.
- soluţia aleasă pentru arhitectura bazei de date este cea adecvată (varianta baza de date centralizată sau bază de date distribuită). În cazul bazelor de

date distribuite auditorul va analiza dacă s-a realizat o corectă şi eficientă distribuire a datelor în nodurile rețelei. Auditorul va determina în ce măsură s-a ținut seama de respectarea următoarelor cerințe:

- nevoile de informare identificate pentru utilizatorii locali;
- asigurarea unui transfer minim al datelor prin rețea;
- necesitatea protecției datelor transferate prin rețea.

Controlul prelucrărilor

În derularea procedurilor de control al prelucrărilor auditorul va trebui să țină seama de:

➢ **tipologia sistemului informatic**:
- sisteme de procesare a tranzacțiilor (TPS – Transaction Processing Systems);
- sisteme destinate conducerii curente (MIS – Management Information Systems);
- sisteme suport de decizie (DSS – Decision Support Systems);
- sisteme destinate conducerii strategice (EIS – Executive Support Systems);
- sisteme pentru automatizarea lucrărilor de birou (OAS – Office Automation Systems).

➢ **natura prelucrărilor**:
În cadrul TPS-urilor, de exemplu, pot fi identificate proceduri de: actualizare a bazei de date, sortare, calcul, regăsirea şi afişarea datelor, generare de rapoarte, grafice etc., salvare şi restaurare a bazei de date;

➢ **nivelul de descentralizare a prelucrărilor**

➢ **modalitățile de introducere a datelor în sistem şi procesarea acestora**:
- introducere pe loturi – procesare pe loturi;
- introducere on line – procesare pe loturi;
- introducere on-line – procesare on-line.

Metode de procesare a datelor

Introducere pe loturi/procesare pe loturi

Această metodă se caracterizează prin faptul că se acumulează documente de un anumit tip (intrările privesc acelaşi tip de tranzacții) şi apoi se procedează la introducerea şi prelucrarea lotului respectiv de date. Procesarea unor tranzacții similare asigură eficiență prelucrării. Procesarea pe loturi se realizează la momente de timp predefinite (zilnic, săptămânal, lunar sau chiar de mai multe ori în cadrul

aceleiaşi zile), periodicitatea fiind determinată de numărul tranzacţiilor şi de natura datelor supuse prelucrării.

Un alt avantaj al metodei este reprezentat de posibilitatea utilizării unor controale care să verifice corectitudinea şi completitudinea prelucrărilor. Se pot utiliza în acest sens următoarele tipuri de controale: controlul totalurilor (se realizează o însumare a valorilor pentru tranzacţiile respective, înaintea procesării, iar acest total se compară cu cel generat automat ca urmare a procesării tranzacţiilor), controlul secvenţialităţii, fiecare tranzacţie având un număr atribuit în cadrul lotului din care face parte.

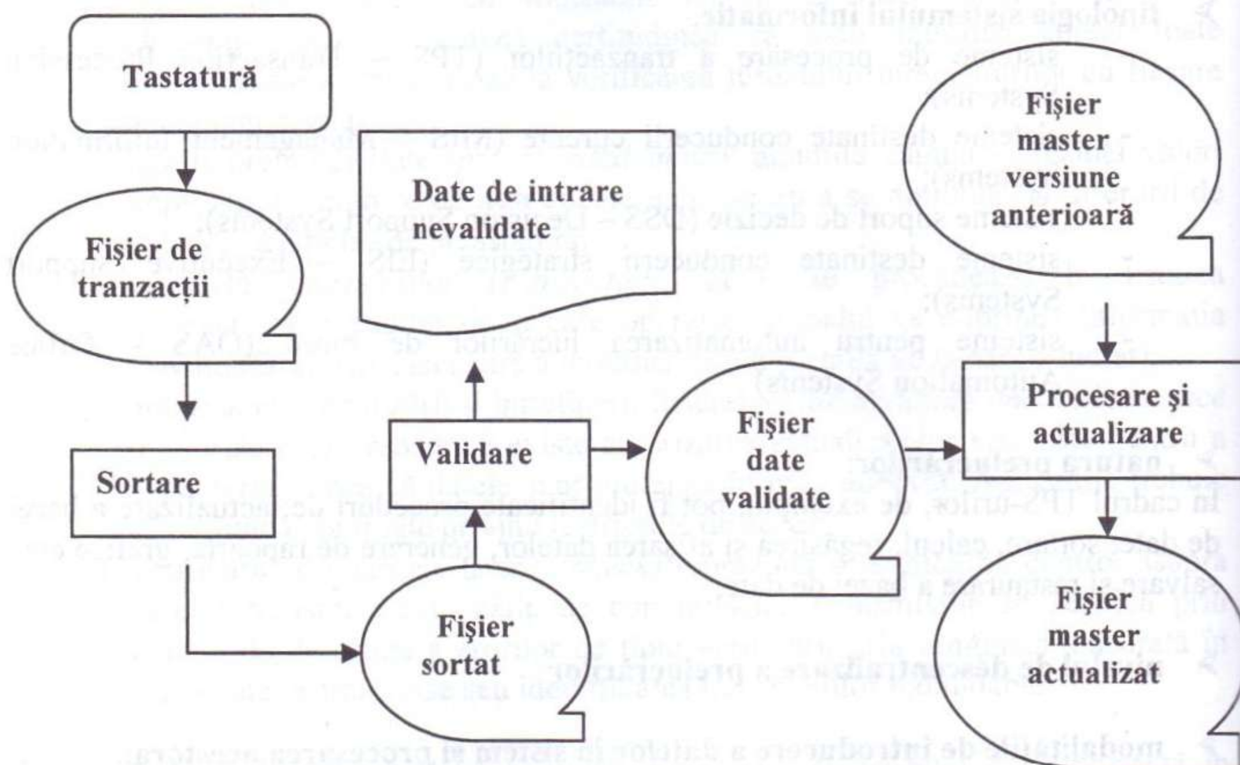


Figura 3.4.3.1. **Introducere şi procesare pe loturi**

Intrări on-line/procesare pe loturi

În cazul acestei metode de procesare datele se introduc direct, pe măsură ce se primesc documentele primare. Datele se validează pe măsură ce sunt introduse de la tastatură şi stocate într-un fişier de tranzacţii temporar pe baza căruia se va proceda la actualizarea periodică a fişierului master.

Avantajul metodei este reprezentat de faptul că validarea datelor se realizează imediat după introducerea acestora, mesajele de eroare fiind afişate operatorului. În cazul introducerii unor date incorecte (de exemplu: omisiuni sau inversiuni de caractere pentru codul clientului sau al unui produs) sau incomplete, în funcţie de mesajele de

eroare afişate, operatorul reintroduce datele. Un alt avantaj este reprezentat de posibilitatea utilizării controalelor de total şi secvenţialitate prezentate şi în cazul metodei anterioare.

Metoda intrări on-line/procesare pe loturi prezintă două variante:

- introducere on-line cu validare imediată şi acces la fişierul master cu prelucrări periodice ale lotului de date introdus (figura 3.4.3.2[6]);
- introducere on-line cu validare imediată fără acces la fişierul master şi procesare periodică a lotului de date introduse (figura 3.4.3.3[7]).

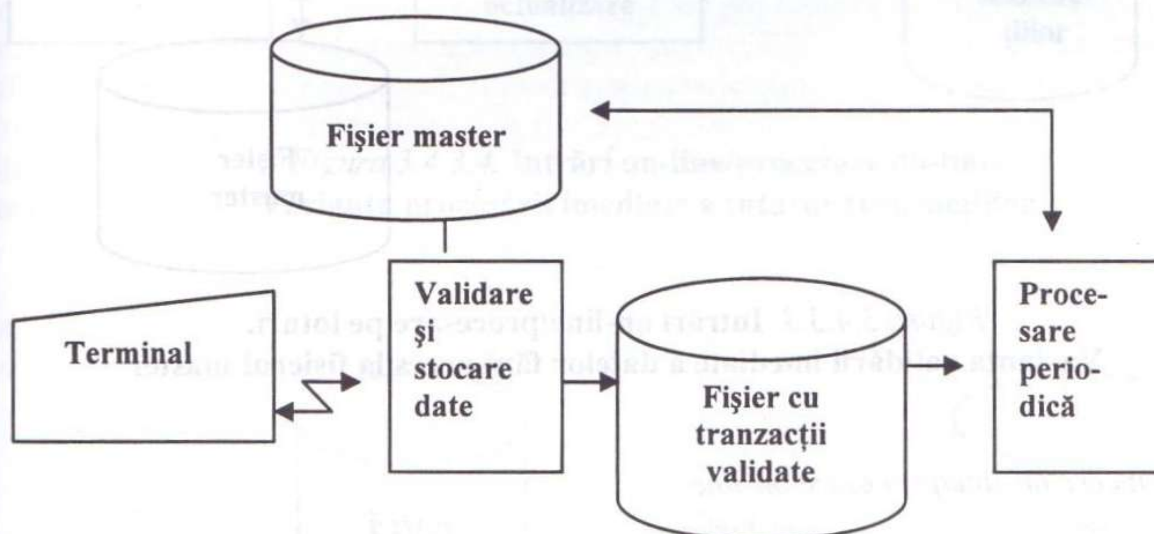


Figura 3.4.3.2. **Intrări on-line/prelucrare pe loturi Varianta validării imediate cu acces la fişierul master**

[6] Graham Cosserat, *Modern Auditing*, John Wiley & Sons Inc, 1996.
[7] Idem.

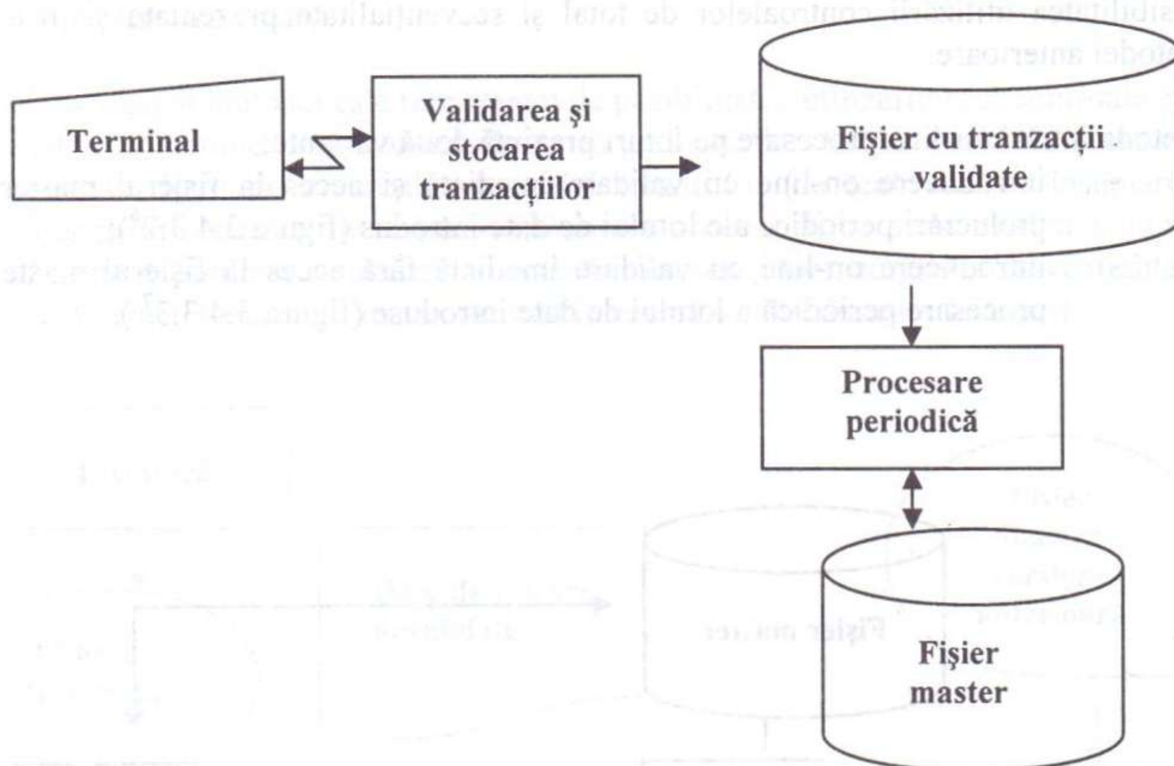


Figura 3.4.3.3. **Intrări on-line/procesare pe loturi. Varianta validării imediate a datelor fără acces la fişierul master**

Introducere on-line/procesare on-line

Această metodă se deosebeşte de metoda intrări on-line/prelucrare pe loturi prin următoarele:

- fişierele master se actualizează pe măsura introducerii datelor;
- se creează un log al tranzacţiilor al cărui rol este de a înscrie cronologic toate tranzacţiile cu scopul de a oferi posibilitatea urmăririi tranzacţiilor, fiecare dintre acestea având asignat un număr unic.

Această metodă mai este cunoscută şi sub numele de *on-line real time* (OLRT). Principalul dezavantaj al metodei este reprezentat de riscul erorilor care pot apărea în fişierul master în cazul unei erori hardware. Soluţia pentru minimizarea acestor riscuri constă în introducerea on-line a intrărilor şi memorarea actualizărilor fişierului master la momentul introducerii datelor. Aceasta presupune utilizarea unei copii a fişierului master. Jurnalul tranzacţiilor va fi folosit periodic pentru actualizarea fişierului master. Din punctul de vedere al utilizatorului, acest sistem nu este diferit de intrări on-line/ prelucrări on-line deoarece rezultatele procesării sunt disponibile imediat, chiar dacă validarea completă a tranzacţiilor şi actualizarea fişierului master sunt finalizate la un moment de timp viitor.

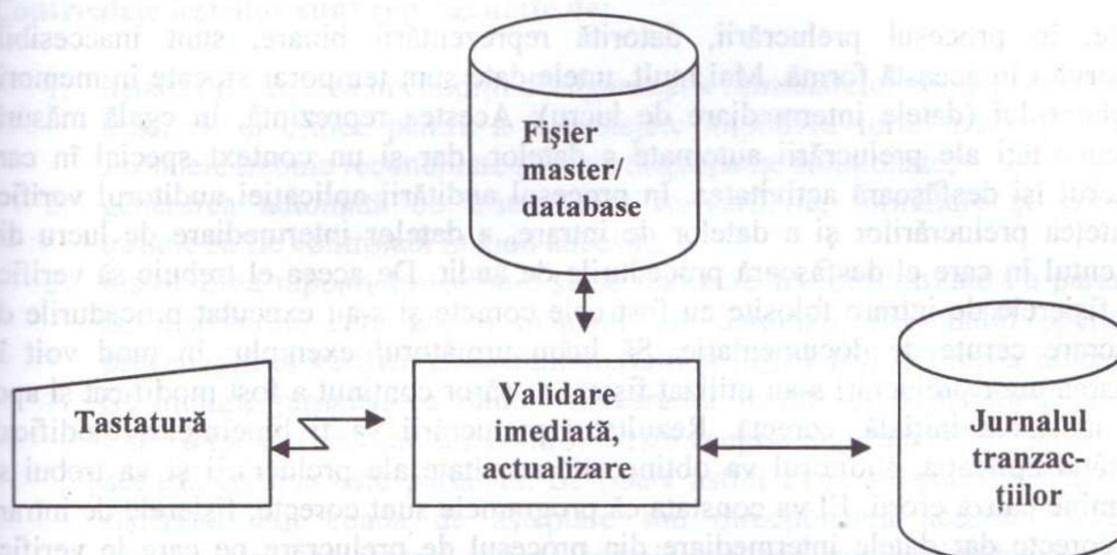


Figura 3.4.3.4. **Intrări on-line/procesare on-line. Varianta procesării imediate a tuturor tranzacțiilor**

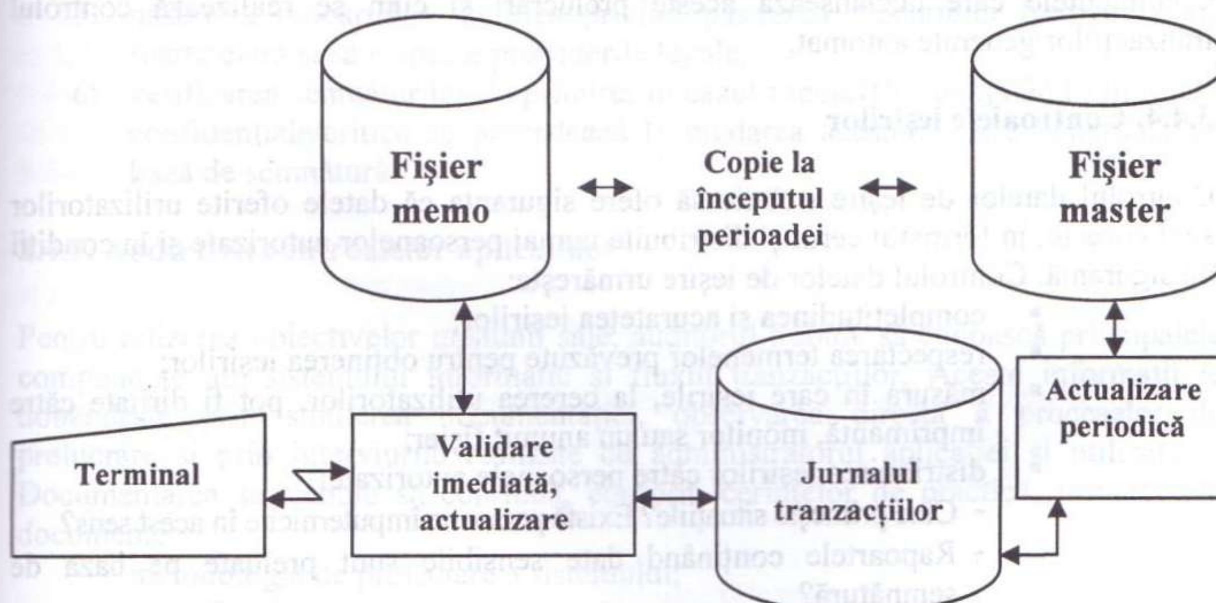


Figura 3.4.3.5. **Intrări on-line/ procesări on-line. Varianta memo updating**

Disponibilitatea datelor

Datele, în procesul prelucrării, datorită reprezentării binare, sunt inaccesibile auditorului în această formă. Mai mult, unele date sunt temporar stocate în memoria calculatorului (datele intermediare de lucru). Acestea reprezintă, în egală măsură, particularităţi ale prelucrării automate a datelor, dar şi un context special în care auditorul îşi desfăşoară activitatea. În procesul auditării aplicaţiei auditorul verifică acurateţea prelucrărilor şi a datelor de intrare, a datelor intermediare de lucru din momentul în care el desfăşoară procedurile de audit. De aceea el trebuie să verifice dacă fişierele de intrare folosite au fost cele corecte şi s-au executat procedurile de prelucrare cerute de documentaţie. Să luăm următorul exemplu: în mod voit în derularea unor prelucrări s-au utilizat fişiere al căror conţinut a fost modificat şi apoi adus la starea iniţială, corectă. Rezultatul prelucrării va fi bineînţeles modificat. Auditând aplicaţia, auditorul va obţine alte rezultate ale prelucrării şi va trebui să determine cauza erorii. El va constata că programele sunt corecte, fişierele de intrare sunt corecte dar datele intermediare din procesul de prelucrare pe care le verifică acum nu sunt aceleaşi cu cele din momentul execuţiei aplicaţiei, când informaţiile generate au fost incorecte. Auditorul va trebui să demonstreze că aplicaţia funcţionând corect fie s-au produs modificări voite în cadrul programelor (care ulterior au fost corectate), fie au fost afectate voit fişierele de intrare.

În cazul prelucrărilor declanşate automat, auditorul trebuie să verifice care sunt evenimentele care declanşează aceste prelucrări şi cum se realizează controlul tranzacţiilor generate automat.

3.4.4. Controalele ieşirilor

Controlul datelor de ieşire trebuie să ofere siguranţa că datele oferite urilizatorilor sunt corecte, în formatul cerut şi distribuite numai persoanelor autorizate şi în condiţii de siguranţă. Controlul datelor de ieşire urmăreşte:

- completitudinea şi acurateţea ieşirilor;
- respectarea termenelor prevăzute pentru obţinerea ieşirilor;
- măsura în care ieşirile, la cererea utilizatorilor, pot fi dirijate către imprimantă, monitor sau un anumit fişier;
- distribuirea ieşirilor către persoanele autorizate:
  - Cine primeşte situaţiile? Există persoane împuternicite în acest sens?
  - Rapoartele conţinând date sensibile sunt preluate pe bază de semnătură?
  - Cum este asigurată protecţia informaţiilor confidenţiale?
- dacă ieşirile către alte aplicaţii se realizează în formatul pe care acestea îl necesită;
- măsura în care se realizează înregistrarea, raportarea şi corectarea erorilor identificate;
- în ce măsură există din partea managementului un control asupra acurateţei ieşirilor şi modului de distribuire a lor.

Controalele ieșirilor sunt reprezentate de:

1. listarea și stocarea în condiții de siguranță a formularelor conținând informații sensibile și critice pentru a fi protejate împotriva furtului sau distrugerii. Jurnalele trebuie reconciliate și orice discrepanțe soluționate;
2. generarea automată de instrumente convertibile, formulare și semnături trebuie să fie controlată în mod adecvat;
3. distribuirea rapoartelor trebuie să se realizeze în conformitate cu parametrii de distribuție, care pot fi manuali sau automați. Personalul operațional procedează la verificarea completitudinii și distribuirii la timp a rapoartelor. Se impune jurnalizarea tuturor rapoartelor înainte de distribuirea acestora. Este totodată necesar un control strict asupra imprimantelor, atunci când această resursă este partajată. Se poate astfel evita ștergerea accidentală a fișierelor din coada de așteptare sau direcționarea acestora spre alte imprimante. Un control riguros trebuie realizat asupra distribuirii fizice a rapoartelor. În cazul rapoartelor conținând date sensibile, trebuie listate în condiții de securiate. În cazul rapoartelor distribuite electronic, trebuie luate măsuri de securizare pe timpul transferului;
4. tratarea erorilor: trebuie stabilite în cadrul aplicației proceduri de raportare și control al erorilor. Lista erorilor trebuie transmisă departamentului care a rulat aplicația pentru a proceda la corectarea acestora;
5. păstrarea rapoartelor: politica privind păstrarea rapoartelor trebuie să fie foarte clară și să respecte prevederile legale;
6. verificarea semnăturilor de primire: în cazul rapoartelor conținând informații confidențiale/critice se procedează la predarea acestora către beneficiar pe bază de semnătură.

3.4.5. Auditarea controalelor aplicațiilor

Pentru relizarea obiectivelor misiunii sale, auditorul trebuie să cunoască principalele componente ale sistemului informatic și fluxul tranzacțiilor. Aceste informații le dobândește prin studierea documentației, observarea directă a proceselor de prelucrare și prin interviurile realizate cu administratorul aplicației și utilizatorii. Documentarea sa trebuie să cuprindă, conform cerințelor de practică, următoarele documente:

- metodologia de proiectare a sistemului;
- specificațiile proiectării funcționale;
- modificările realizate în timp asupra programelor;
- manualele-utilizator;
- documentații tehnice ale furnizorului de software.

Înțelegerea complexității și funcționalității aplicației îi oferă posibilitatea de a-și realiza strategia de teste în vederea evaluării adecvării, completitudinii și eficienței

controalelor. Sarcina auditorului este de a identifica punctele forte ale controalelor, precum şi punctele slabe.

De o deosebită importanţă este diagrama tranzacţiilor, aceasta oferind auditorului informaţii cu privire la principalele controale, punctele de introducere a datelor, procesării şi afişării în vederea evaluării eficienţei controalelor.

Auditorul sistemului informatic include în lista obiectivelor misiunii de audit verificarea respectării principiului segregării funcţiilor incompatibile. În acest sens va proceda la verificarea următoarelor probleme:

1. **separarea funcţiilor**: procesarea automată a datelor, prin caracteristicile sale şi implicaţiile acţiunilor diverşilor utilizatori, impune reguli stricte privind separarea funcţiilor. Următoarele atribuţii nu vor putea fi alocate niciodată unei singure persoane: iniţierea, autorizarea, verificarea şi distribuţia. În egală măsură persoanele implicate în proiectarea, relizarea, actualizarea şi administrarea software-ului nu vor putea avea atribuţii de exploatare curentă a acestuia. Verificarea separării funcţiilor incompatibile se va realiza prin analizarea fişelor posturilor şi verificarea măsurii în care, în activitatea curentă, persoanele respectă atribuţiunile asignate postului;

2. **autorizarea intrărilor**: regula celor „patru ochi" este aplicabilă şi în cazul aplicaţiilor informatice. Drepturile acordate utilizatorilor trebuie să facă demarcaţia între persoanele autorizate să introducă date în sistem şi cele cu drept de autorizare. În cazul autorizărilor în sistem auditorul va trebui să verifice drepturile oferite utilizatorilor şi modul de executare a procedurilor de introducere şi autorizare procedând la efectuarea de teste utilizând un eşantion de documente primare. În cazul autorizării manuale se procedează la verificarea existenţei autorizării pe documentul primar;

3. **balanţe**: sunt executate pentru a verifica controalele de tip total şi modul în care se realizează reconcilierea datelor;

4. **erori de control şi corecţia acestora**: erorile de introducere şi înregistrările respinse trebuie verificate înaintea reintroducerii. Auditorul va proceda la verificarea modului în care managerul a procedat la verificarea erorilor şi autorizarea erorilor plecând de la un eşantion de înregistrări eronate;

5. **distribuirea rapoartelor:** auditorul va trebui să verifice măsura în care generarea şi distribuirea rapoartelor conţinând informaţii confidenţiale se realizează în condiţii de securitate adecvate. Va proceda la metoda observării directe, la verificarea jurnalelor de distribuire pe bază de semnătură a rapoartelor, precum şi la testarea în sistem a drepturilor de acces la funcţiile de generare/vizualizare rapoarte;

6. **testarea drepturilor de acces al utilizatorilor la aplicații:** auditorul trebuie să obțină convingerea că drepturile de acces oferite utilizatorilor la aplicații corespund atribuțiilor lor de serviciu.

3.4.6. Testarea integrității datelor

Verificarea integrității datelor este reprezentat de un set de teste vizând acuratețea, completitudinea, consistența și autorizarea datelor din sistemul informatic. Implică o serie de controale similare celor utilizate la introducerea datelor și indică erorile la introducerea sau procesarea datelor. Atunci când verificarea integrității se realizează în baza documentelor primare (cele care au stat la baza introducerii datelor), nu este necesară verificarea la un anumit moment de timp a întregului fișier.

Există două tipuri de teste pe care considerăm necesar să le amintim: testele de integritate relațională și respectiv testul de integritate referențială. Testul de integritate relațională verifică corelații ale valorilor atributelor. Aceste corelații se realizează prin rutine de validare a datelor sau prin definirea de restricții și caracteristici ale câmpurilor realizate la crearea tabelelor bazei de date. Restricțiile de integritate referențială asigură consistența bazei de date și vizează valorile câmpurilor-chei primare și a câmpurilor-cheie externă definite în baza acestora. Sistemele de gestiune a bazelor de date (SGBD) oferă mecanisme de implementare și control al restricțiilor de integritate referențială.

În cazul sistemelor informatice multiutilizator, SGBD oferă funcția de administrare a accesului concurent al utilizatorilor la datele stocate. Restricțiile de integritate specifice datelor transmise on-line (cunoscute sub numele de ACID) sunt următoarele:

1. **Atomicitatea:** o tranzacție este complet executată sau nu este executată deloc;
2. **Consistența:** toate restricțiile de integritate sunt aplicabile tuturor tranzacțiilor, asigurând trecerea succesivă a bazei de date dintr-o stare consistentă în alta;
3. **Izolarea:** fiecare tranzacție este izolată de celelalte tranzacții;
4. **Durabilitatea:** dacă tranzacția realizată în sistem de către un utilizator a fost salvată nu va fi afectată de erorile soft sau hardware.

În activitatea sa, auditorul utilizează metode și tehnici de analiză a programelor și controalelor aplicațiilor, precum și metode de testare destinate selectării și monitorizării procesării tranzacțiilor. În cele ce urmează, vom enunța principalele tehnici și metode pentru categoriile de teste enunțate.

1. **Analiza programelor aplicațiilor**

- *snapshot*: verifică logica programului. Se apelează la un flux de date pentru a se urmări logica procesului de procesare;

- *maparea*: Permite analizarea programului în timpul execuţiei pentru a verifica măsura în care sunt executate liniile de cod. Identifică potenţialele expuneri datorate soluţiei de programare;
- *tracing and tagging*: tehnica de *tracing* permite urmărirea „traseului" instrucţiunilor executate în cadrul aplicaţiei. Tehnica de **tagging** permite marcarea tranzacţiilor care apoi urmează a fi urmărite prin tehnica de *tracing*.

2. **Testarea controalelor aplicaţiilor**

- *test data/deck*: permite o modalitate obiectivă de revizuire a controalelor programului. Scopul urmărit este de a simula „traseul" tranzacţiilor în cadrul programului (ce linii de cod se execută);
- *evaluarea sistemului bazată pe teste (base-case system evaluation)* reprezintă o modalitate de testare cuprinzătoare a programului. În acest scop se utilizeată seturi de date de test pregătite special pentru acest scop;
- *operare paralelă*: constă în procesarea simultană a datelor curente pe sistemul operaţional şi pe sistemul nou şi compararea rezultatelor prelucrării generate de cele două sisteme;
- *testarea integrată (integrated testing facility)*: creează un fişier fictiv cu tranzacţii de test care se vor prelucra simultan cu date reale;
- *simulare paralelă*: prelucrarea datelor curente se realizează prin programe care simulează logica aplicaţiei. Prezintă avantajul de a nu necesita date de test;
- *programe de selectare a tranzacţiilor (transaction selection programs)*: implică utilizarea unui software de audit pentru vizualizarea şi selectarea tranzacţiilor introduse în aplicaţia curentă.

3. **Selectarea şi monitorizarea procesării tranzacţiilor**

- *colecţii de date de audit imbricate (embeded audit data collection)*: soft de audit imbricate în programele calculatorului selectând tranzacţii introduse şi generând tranzacţii. Oferă eşantioane şi statistici.
- *înregistrări extinse (extended records)*: tehnică permiţând crearea unui fişier care conţine ansamblul datelor care au fost afectate de acelaşi program.

3.4.7. Auditul continuu online

Reprezintă o tehnică de audit modernă specifică sistemelor de e-business, permiţând auditorului strângerea dovezilor privind credibilitatea sistemului în baza monitorizării continue a procesării. Această tehnică implică utilizarea de instrumente informatice de audit specifice mediilor informatice cărora le este caracteristică partajarea timpului şi procesarea unor volume mari de date fără a furniza/furnizând puţină informaţie pe suport hârtie.

Tehnicile de audit specifice auditului on-line sunt:

1. *systems control audit review file and embedded audit modules (SCARF/EAM)*: implică instalarea software-ului de audit special realizat în aplicația host de auditat astfel încât aplicația este monitorizată selectiv;
2. *snapshots*: permite urmărirea tranzacțiilor de la inițiere până la finalul procesării;
3. *audit hooks*: tehnică permițând intervenția auditorului înainte ca o eroare sau iregularitate să iasă de sub control;
4. *integrated test facility* (*ITF*- facilitate de test integrată): tehnică permițând procesarea în sistemul auditat atât a datelor reale, cât și a datelor de test, în funcție de intervenția auditorului, urmând ca auditorul că evalueze rezultatele procesării;
5. *continous and intermitent simulation* (CIS - simulare continuă și intermitentă): tehnica permite selectarea tranzacțiilor îndeplinind anumite criterii de selecție și aplicarea simulării execuției prelucrării asupra lor.

3.5. Dezvoltarea infrastructurii TI

Infrastructura TI la nivelul unei organizații este reprezentată de ansamblul serviciilor, echipamentelor hardware și software folosite pentru stocarea, procesarea, transmiterea și afișarea informațiilor din cadrul sistemului informatic. Extinderea continuă a noilor tehnologii informaționale în cadrul marilor organizații a condus adesea la infrastructuri informatice complexe și neomogene. Evoluția mediului informațional actual este una naturală la care mediul de afaceri trebuie să se adapteze, să integreze cele mai bune tehnici și instrumente care să-i ofere transparență și datele necesare pentru a determina, spre exemplu, care sunt prioritățile în dezvoltarea proiectelor TI, în realizarea investițiilor astfel încât acestea să susțină obiectivele organizației și să aducă un plus de valoare.

Infrastructura TI la nivelul unei organizații trebuie să asigure realizarea următoarelor caracteristici:

- *flexibilitatea* – astfel încât aceasta să permită adaptarea la noile tehnologii care apar;
- *scalabilitatea* – platforma TI trebuie să permită extinderea cu ușurință a infrastructurii proporțional cu creșterea afacerii;
- *robustețea* – parametru ce oferă garanția stabilității, disponibilității și securității sistemului informatic;
- *ușurința operării* - productivitatea și costurile instruirii personalului depind foarte mult de acest aspect;
- *administrarea*;
- *timpul necesar implementării*;
- *aplicațiile disponibile*;
- *compatibilitatea cu aplicațiile, sistemele curente.*

În general, nevoia dezvoltării infrastructurii TI poate fi realizată din următoarele motive:

- pentru îmbunătăţirea funcţionalităţii sistemului în ceea ce priveşte timpul de răspuns, prezenţa unor erori de program;
- pentru creşterea eficienţei exploatării sistemului: perfecţionări privind administrarea reţelei, a bazelor de date;
- pentru perfecţionarea securităţii sistemului realizată în primul rând prin identificarea vulnerabilităţilor sistemului şi corectarea acestora;
- pentru corectarea erorilor semnalate determinate de frecvenţa crescută a incidentelor, inclusiv căderi de sistem;
- actualizări de rutină impuse de producătorii de software la modificarea versiunii aplicaţiilor din sistem;
- noi cerinţe funcţionale pentru utilizatorii finali determinate de schimbări legislative, schimbări ale orientării afacerii.

Procesul de dezvoltare/achiziţionare a infrastructurii TI se realizează în trei etape:

- analiza arhitecturii fizice;
- planificarea implementării noii arhitecturi;
- întreţinerea noului sistem.

La nivelul primei etape, ***de analiză a arhitecturii fizice,*** se va verifica dacă decizia de dezvoltare este în conformitate cu obiectivele şi planurile organizaţiei şi, de asemenea, dacă au fost determinate costurile şi beneficiile care vor rezulta din acest proces. În acest sens, se va urmări:

- analiza infrastructurii existente;
- proiectarea unei noi arhitecturi, ţinând cont de arhitectura existentă, cât şi de constrângerile particulare ale organizaţiei, cum ar fi:
    - reducerea costurilor;
    - creşterea funcţionalităţilor;
    - breşele de securitate si confidenţialitate.
- descrierea cerinţelor funcţionale ale noii arhitecturi;
- dezvoltarea unui prototip bazat pe aceste cerinţe funcţionale.

Prin urmare, rezultatul acestei etape îl constituie prototipul, care, în urma testării, va genera cea de-a doua etapă ***planificarea implementării infrastructurii.***

Decizia privind implementarea efectivă a noii arhitecturi implică analiza următorilor factori:

- impactul potențial asupra sistemului informatic și asupra serviciilor furnizate utilizatorilor: capacitate, securitate, timp de răspuns al sistemului, performanță;
- efectul neimplementării noii arhitecturi;
- resursele necesare pentru implementare (costuri, personal);
- cerințe pentru resursele viitoare, dacă se va implementa noua arhitectură.

La baza desfășurării acestei etape stau proceduri clare de implementare a noului sistem, ele fiind asociate următoarelor faze:

- procesul de achiziționare a componentelor (hardware/software) necesare implementării;
- timpul de livrare;
- planul de instalare;
- testarea instalării.

Implementarea noii arhitecturi se bazează, în mod practic, pe achiziția de noi componente hardware și/sau software. Pe lângă stabilirea unor criterii clare în ceea ce privește selecția echipamentelor și a furnizorilor, procesul de achiziție presupune cunoașterea echipamentelor și software-ului disponibil pe piață, transmiterea cererilor de ofertă către potențialii furnizori, evaluarea ofertelor, participarea la licitații, negocierea contractului, achiziția și instalarea echipamentelor și software-ului. Spre exemplu, specificațiile care vor fi adresate furnizorilor în cazul achiziției de echipamente hardware vor include:

- descrierea structurii sistemului informatic (centralizate sau descentralizate, distribuite);
- cerințele de procesare a datelor, precum sistemele de aplicații existente, cerințele de performanță, abordarea procesării (sisteme client-server, on-line/pe loturi, baze de date în timp real etc.);
- cerințele hardware, care vizează caracteristici legate de viteză de procesare, spațiu de memorare, perifericele asociate, capacitatea rețelei, numărul de terminale și nodurile pe care sistemul este nevoit să-l susțină;
- aplicațiile software, cum ar fi sistemul de operare, compilatoarele, librăriile de program, software de comunicație, sistemele de gestiune a bazelor de date, software-ul de control al accesului;

- cerinţe auxiliare, precum sisteme de întreţinere, training, bakup;
- cerinţe de adaptabilitate: posibilitatea de actualizare, compatibilitatea cu platforma existentă, capacitatea de schimbare cu alte echipamente;
- constrângeri legate de nivelul personalului, date de livrare, capacitatea hardware existentă;
- cerinţe de conversie precum: timpul de testare a echipamentului hardware, facilităţi de conversie a sistemului, planificarea costurilor.

Odată achiziţionate şi instalate, echipamentele şi software-ul trebuie testate pentru a se verifica performanţele acestora cu specificaţiile tehnice înscrise în manualele de utilizare. Chiar dacă noua arhitectură a fost implementată şi dată în exploatare, este necesară o **analiză postimplementare** pentru a se verifica realizarea beneficiilor scontate sau apariţia unor noi oportunităţi de dezvoltare a sistemului.

Întreţinerea sistemului

Imediat ce sistemul a fost implementat, urmează o nouă etapă: întreţinerea acestuia. Dinamica mediului în care operează organizaţia, cât şi complexitatea sistemului implementat vor constitui factori care influenţează costul întreţinerii acestui sistem. Volatilitatea informaţiilor, concurenţa acerbă de pe piaţă pot determina schimbări ale infrastructurii TI. În acest sens, un aspect important la nivelul acestei etape îl reprezintă procesul de management al modificărilor ce se impun. Procesul va debuta cu autorizarea modificărilor care sunt necesare. Se impune apoi dezvoltarea unei metodologii pentru a se identifica priorităţile de schimbare şi efectele generate de acestea. Apoi, ciclul se reia şi procesul continuă cu testarea noilor modificări, actualizarea documentaţiei care adesea din constrângeri de timp şi resurse este neglijată.

În general, modificările din cadrul unui SI, care vizează componentele hardware, software (sistem de operare, utilitare), cât şi aplicaţiile individuale, pot avea un impact semnificativ asupra controalelor existente şi pot afecta fundamental funcţionalitatea sistemului. Indiferent de amploarea acestui proces, efectele asupra operării sistemului trebuie să fie minime, pentru a nu perturba activitatea curentă a organizaţiei. Mai mult, aceste schimbări ale infrastructurii TI vor determina modificarea planurilor de recuperare în caz de dezastre, pentru asigurarea continuităţii activităţii.

La nivelul organizaţiei, procedurile de control al schimbărilor vor urmări:
- analiza procedurilor de autorizare de către management;

- documentarea și planificarea calendaristică a oricărei modificări aduse sistemului inițial;
- testarea software-ului modificat înainte de a fi utilizat în mediul de producție;
- examinarea efectelor schimbării;
- pregătirea unui plan de recuperare, chiar dacă sistemul funcționează corect;
- elaborarea și implementarea procedurilor privind schimbările de urgență; schimbările de urgență se referă la căderea completă a sistemului, fapt ce impune asigurarea funcțiilor critice pentru continuitatea activității.

3.6. Auditul dezvoltării, achiziției și întreținerii SI

Dezvoltarea sau achiziția unui sistem informatic este o activitate amplă, complexă, responsabilitatea ei fiind atribuită unui manager de proiect. Auditorul TI își poate exercita atribuțiile fie ca membru al echipei de proiectare, dezvoltare a proiectului, fie în cadrul unei misiuni de audit, în cursul căreia, în cadrul organizației, se realizează un nou proiect.

În general, acesta va realiza:

- analiza componentelor principale, obiectivele sistemului existent și a cerințelor utilizatorilor pentru a identifica ariile care solicită controale;
- determinarea și ierarhizarea riscurilor majore ale sistemului prin discuții cu membrii echipei de proiectare și dezvoltare pentru a permite selectarea de controale;
- identificarea controalelor necesare pentru a reduce riscurile din sistem;
- consilierea cu membrii echipei de dezvoltare privind procesul de proiectare a noului sistem și implementarea controalelor necesare prin evaluarea celor existente;
- monitorizarea procesului de dezvoltare a sistemului pentru a se asigura că aceste controale sunt implementate, cerințele utilizatorilor sunt atinse;
- participarea la analiza postimplementare;
- evaluarea standardelor și celor mai bune practici de întreținere a sistemelor informatice;
- testarea procedurilor de întreținere pentru a se asigura că ele au fost aplicate în conformitate cu aceste standarde;

- evaluarea procedurilor de întreţinere a sistemului pentru a determina dacă obiectivele de control au fost atinse prin analiza rezultatelor testelor desfăşurate şi a altor probe de audit;
- evaluarea securităţii bibliotecilor de programe pentru a se asigura integritatea resurselor şi testarea controalelor existente.

Intervenţia auditorului TI se face simţită pe tot parcursul procesului, acţiunile sale fiind relevate la nivelul fiecărei etape.

3.7. Test de evaluare a cunoştinţelor

1. Motivul principal pentru separarea testelor de mediu de dezvoltare este:
   a. accesul restricţionat la sistemele aflate sub test;
   b. separarea utilizatorilor de personalul ce dezvoltă aplicaţia;
   c. controlul stabilităţii mediului de testare;
   d. accesul securizat la sisteme în timpul dezvoltării.

2. O societate şi-a stabilit un comitet de coordonare pentru a supraveghea programul de e-business. Comitetul de coordonare ar trebui cel mai probabil să fie implicat în:
   a. documentarea cerinţelor;
   b. parcurgerea etapelor proiectului;
   c. proiectarea controalelor de interfaţă;
   d. specificarea rapoartelor.

3. Care dintre următoarele faze reprezintă punctul optim pentru atingerea liniilor de bază ale software-ului:
   a. testarea;
   b. proiectarea;
   c. stabilirea cerinţelor;
   d. dezvoltarea.

4. Responsabilitatea pentru proiectare, implementare şi întreţinere a unui sistem de controale interne revine:
   a. auditorului SI;
   b. conducerii;
   c. auditorului extern;
   d. personalului care realizează programe (programatorului).

5. O validare a editării datelor care verifică concordanța dintre datele de intrare și un număr de apariții predeterminat este:
   a. control limită;
   b. control rezonabil;
   c. control de domeniu;
   d. control de valabilitate.

6. Înainte de implementarea controalelor conducerea trebuie să se asigure mai întâi că acestea:
   a. satisfac cerințele în domeniul problemelor de risc;
   b. nu reduc productivitatea;
   c. sunt bazate pe analiza cost – beneficiu;
   d. sunt detective sau corective.

7. Care dintre următoarele afirmații reprezintă cel mai mare risc la implementarea depozitelor de date:
   a. creșterea timpului de răspuns în sistemele de producție;
   b. controalele de acces ce nu sunt adecvate pentru a preveni modificarea datelor;
   c. duplicarea datelor;
   d. date care nu sunt curente sau actualizate.

8. Un sistem de asistare a deciziei:
   a. este folosit pentru rezolvarea problemelor bine structurate;
   b. reprezintă combinarea utilizării modelelor cu metode de acces netradițional la date și funcții de regăsire;
   c. crește flexibilitatea în luarea deciziei de către utilizatori;
   d. sprijină numai luarea deciziilor structurate.

9. Pentru a cumpăra un pachet de programe software, conducerea companiei solicită părerea auditorului SI în evaluarea riscului. Care dintre următoarele afirmații reprezintă un risc major?
   a. indisponibilitatea codului-sursă;
   b. lipsa certificatului de calitate al furnizorului;
   c. absența referințelor vânzătorului/clientului;
   d. experiența redusă a vânzătorului în utilizarea pachetului.

10. Când evaluează portabilitatea aplicaţiilor care utilizează baze de date auditorul SI trebuie să verifice:
   a. utilizarea SQL;
   b. existenţa informaţiilor privind proceduri de import-export cu alte sisteme;
   c. utilizarea indecşilor;
   d. toate entităţile au nume semnificative şi sunt identificate prin chei primare şi chei externe.

Capitolul 4

Infrastructura tehnică a sistemului informațional

Capitolul 4
Infrastructura tehnică a sistemului informațional

4.1. Noțiuni generale

Ca auditorul SI să evalueze concordanța dintre managementul serviciilor IT și obiectivele companiei, acesta trebuie să înțeleagă infrastructura tehnică pe care se bazează SI, care are două componente principale: sistemele de calcul și rețelele de calculatoare. Capitolul 4 încearcă, printr-un limbaj descriptiv și mai puțin tehnic, să familiarizeze auditorul SI cu principalele concepte, procese și proceduri privind infrastructura tehnică a SI, care reprezintă unul dintre domeniile auditului SI.

Sistemele de calcul existente funcționează după o arhitectură secvențială, cunoscută sub numele de arhitectura Von Neumann, potrivit căreia o problemă care urmează să fie rezolvată este descompusă în operații elementare care apoi se ordonează secvențial pentru a fi prelucrate de calculator. Modelul topologic de bază (figura 4.1.1) scoate în evidență elementele structurale fundamentale, atât cele fizice (*resurse de calcul* - C, *resurse de memorare* - M), *echipamente de intrare/ieșire* - I/E, *circuitele care asigură transmisia informației între componente* - T), cât și pe cele logice (*sistem de operare*, *programe utilitare)*.

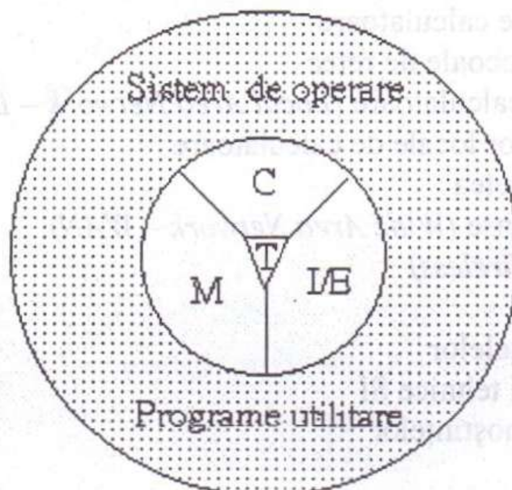


Figura 4.1.1. **Modelul unui sistem de calcul**

Un **sistem de calcul** reprezintă o colecție de resurse **hardware** (unitatea centrală de prelucrare - UCP, memoria, dispozitivele periferice de intrare/ieșire) și **software** (sistem de operare, programe utilitare) care interacționează în vederea satisfacerii cerințelor utilizatorilor.

4.2. Hardware-ul SI

4.2.1. Unitatea centrală de prelucrare

Componenta principală a unui calculator este unitatea centrală de prelucrare (UCP), care, în cazul unui microcalculator, se numeşte microprocesor şi este localizată pe placa de bază a acestuia (figura 4.2.1).

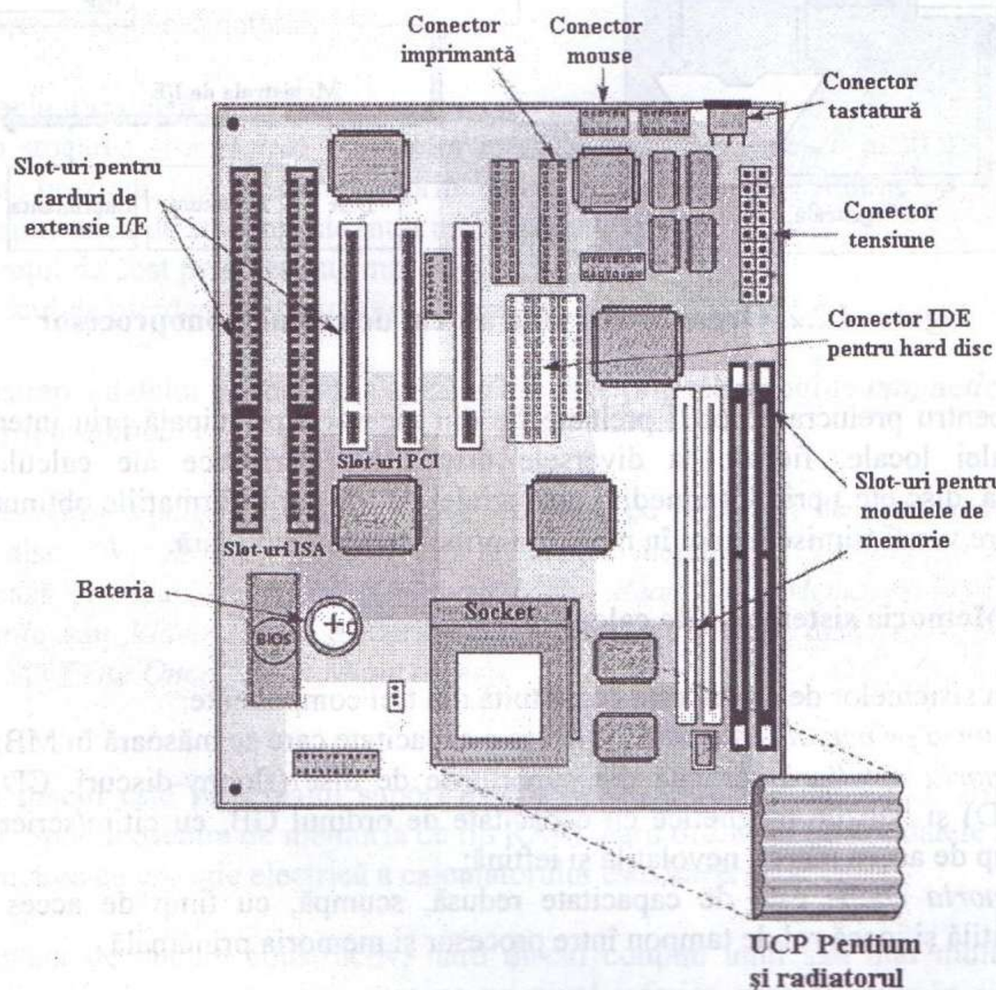


Figura 4.2.1 **Placa de bază (Intel Pentium)**

UCP este formată din trei componente principale:

- *unitatea aritmetico-logică* (UAL): are rolul de a executa operaţiile aritmetice şi funcţiile logice;
- *unitatea de control*: urmăreşte extragerea instrucţiunilor din memoria principală, decodificarea acestora, identificarea operanzilor şi, dacă este cazul, transferul lor în registrele UCP, execuţia instrucţiunilor şi scrierea rezultatelor în memoria principală;
- un *ansamblu de registre*: constituind o memorie locală, de dimensiune redusă şi foarte rapidă.

În funcţie de numărul UCP-urilor, sistemele de calcul pot fi de tip: *monoprocesor* (figura 4.2.2) sau *multiprocesor*.

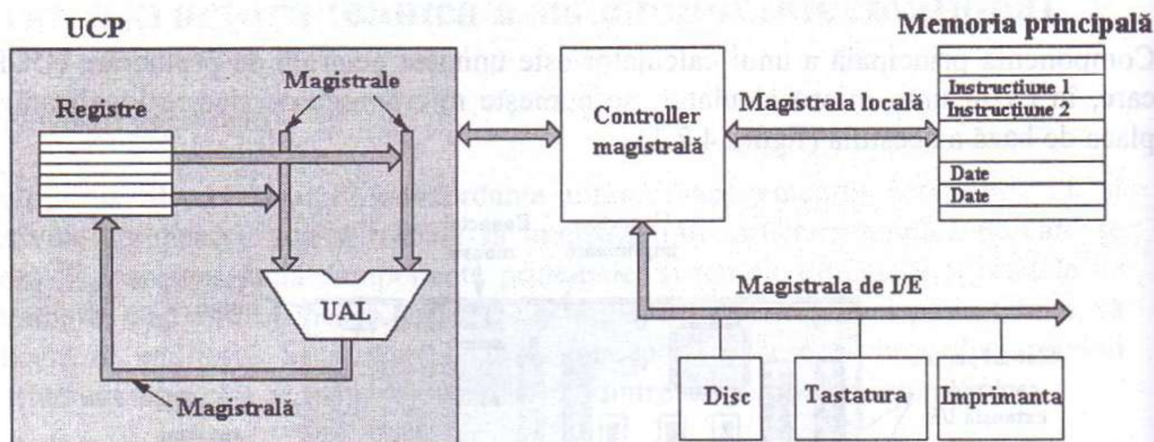


Figura 4.2.2 **Organizarea unui sistem de calcul monoprocesor**

Datele pentru prelucrare pot fi preluate fie din memoria principală prin intermediul magistralei locale, fie de la diversele dispozitive periferice ale calculatorului (tastatură, disc etc.) prin intermediul magistralei de I/E, iar informaţiile obţinute după prelucrare vor fi trimise înapoi în memoria principală sau auxiliară.

4.2.2. Memoria sistemelor de calcul

Memoria sistemelor de calcul este constituită din trei componente:

- *memoria principală* este volatilă şi are o capacitate care se măsoară în MB;
- *memoria auxiliară* formată din suporturile de disc (floppy-discuri, CD-ROM, DVD) şi benzile magnetice cu capacitate de ordinul GB, cu citire/scriere lentă (timp de acces mare), nevolatilă şi ieftină;
- *memoria cache* este de capacitate redusă, scumpă, cu timp de acces redus, volatilă şi joacă rol de tampon între procesor şi memoria principală.

Memoria principală are rolul de a stoca programele şi datele pe parcursul execuţiei acestora. Aceasta este constituită dintr-o succesiune de locaţii care sunt identificate prin adrese fizice. Numărul total al locaţiilor adresabile care pot fi accesate de procesor reprezintă **capacitatea memoriei,** care se exprimă în kilobytes (1 KB=2^{10} bytes), megabytes (1 MB=2^{10} KB), gigabytes (1 GB=2^{10} MB) sau terabytes (1 TB=2^{10} GB). **Timpul de acces** la memorie este intervalul de timp ce separă cererea unei informaţii de obţinerea acesteia şi se măsoară în nanosecunde.

După posibilitatea modificării conţinutului, memoria principală a calculatoarelor poate fi constituită din memorie de tip **RAM** (***Random Access Memory***) şi **ROM**

(*Read Only Memory*). În sistemele moderne RAM-ul este instalat în module **SIMM** (*Single In-line Memory Modules*), care lucrează pe opt biţi sau **DIMM** (*Dual In-Line Memory Modules*), care lucrează pe 64 de biţi.

În ultima perioadă se utilizează în mod frecvent ***memoria flash*** (*flash memory*), care se comportă ca memoria de tip RAM, dar păstrează conţinutul, chiar dacă este întreruptă tensiunea de alimentare. ***USB*** (*Universal Serial Bus*) ***Flash Drive*** este un dispozitiv de memorare portabil, recunoscut de sistemele de operare, care permite accesarea şi stocarea datelor.

Memoria auxiliară

Pentru stocarea şi regăsirea volumelor mari de date se utilizează memoria auxiliară. Aceasta prezintă, faţă de memoria principală, următoarele trei avantaje:

- capacitatea de stocare este mult mai mare;
- preţul de cost pe octet este mai mic;
- riscul de pierdere a informaţiei este redus.

Înregistrarea datelor pe memoria auxiliară se face prin tehnologiile ***magnetică***, ***optică*** şi ***magneto-optică***.

Prin *tehnologia magnetică* se înregistrează date pe suporturi de tipul: disc flexibil, hard disc (Winchester), discuri zip şi bandă magnetică. *Tehnologia optică* se utilizează în cazul: CD-ROM (*Compact Disk - Read Only Memory*), DVD (*Digital Versatile* sau *Video Disk*), discurile magneto-optice (MO), discurile optice de tip WORM (*Write Once, Read Many times*).

Hard discul este principalul suport extern de memorare a datelor în sistemele de calcul. Spre deosebire de memoria de tip RAM, hard discul va păstra datele şi după ce alimentarea cu energie electrică a calculatorului este întreruptă.

Din punct de vedere constructiv, hard discul conţine unul sau mai multe discuri, împărţite în piste concentrice care pe un nivel inferior sunt divizate în sectoare de lungime fixă.

CD-ROM (*Compact Disk - Read Only Memory*) este un mediu de memorare optic, spre deosebire de hard discuri sau discurile fexibile, care utilizează tehnologia magnetică. CD-ROM-ul este inscripţionat cu ajutorul unei raze laser care produce mici denivelări, prin ardere, în suprafaţa mediului folosit, pe o pistă în spirală. Citirea se realizează tot cu o rază laser.

Unităţile **DVD** (*Digital Video Disk /Digital Versatile Disk*) oferă mai mult spaţiu de stocare şi o viteză de transfer mai mare decât CD-ROM-urile.

Benzile magnetice sunt utilizate pentru realizarea copiilor de rezervă (backup) sau pentru transportarea unor volume mari de date de la un calculator la altul.

USB (***Universal Serial Bus***) este o magistrală serie care permite conectarea a 127 de periferice diverse (adaptoare, CD-RW, DVD-RW, scanner, cameră web, hub, hard disc etc.) conectate la un singur canal. În plus, permite recunoaşterea automată a perifericelor conectate pe canal şi determinarea driver-ului necesar în funcţionare. Pe o astfel de magistrală, informaţiile codificate în NRZI (*Non Return to Zero Inverted*) pot circula la un debit adaptat perifericului (rata de transfer de până la 480 Mbps). USB utilizează principiile de funcţionare similare celor din reţelele locale.

4.2.3. Clasificarea sistemelor de calcul

Clasificarea sistemelor de calcul se poate face luând în considerare următoarele criterii: *tipul unităţii centrale de prelucrare, capacitatea memoriei principale, capacitatea de stocare a memoriei auxiliare, viteza perifericelor de ieşire, viteza de prelucrare exprimată în milioane de instrucţiuni pe secundă (mips), numărul de utilizatori care pot avea acces simultan, costul sistemului.*

Având în vedere totalitatea criteriilor enumerate mai sus, calculatoarele sunt, în general, grupate în următoarele categorii de bază: *microcalculatoare, minicalculatoare, mainframe* şi *supercalculatoare*. Este dificil să se asocieze o definiţie fiecărei categorii, ţinând seama de progresele tehnologice şi de rapiditatea cu care se pot schimba parametrii de mai sus. Totuşi, fiecare categorie deţine o serie de caracteristici proprii, care le individualizează în comparaţie cu celelalte.

Microcalculatorul, identificat adesea cu un calculator personal (PC) reprezintă tipul de calculator care utilizează un microprocesor ca unitate centrală de prelucrare (UCP) şi poate fi folosit numai de o singură persoană la un moment dat.

Staţiile de lucru (workstations) sunt calculatoare puternice dedicate unui singur utilizator; sunt recomandate pentru aplicaţiile complexe, cum ar fi proiectarea de produse software şi animaţia pe calculator; în mod frecvent, sunt utilizate ca suport pentru servere de reţea sau servere în internet.

Calculatoarele de birou *(desktop computers)* sunt cele mai obişnuite tipuri de PC-uri. *Calculatoarele notebook* (*laptop*) sunt utilizate de persoanele care au nevoie de performanţele unui sistem desktop, dar să fie portabil (greutate redusă, alimentarea la tensiune normală sau existenţa unei baterii reîncărcabile); sunt foarte practice deoarece funcţionează în acelaşi fel ca sistemele desktop, folosind aceleaşi pachete de programe.
Calculatoarele personale utilizează diverse versiuni ale sistemelor de operare UNIX şi Microsoft Windows sau un alt sistem de operare similar, cum ar fi Apple Macintosh.

Sistemele PC sunt folosite pentru aplicațiile standard din activitatea de birou, cum ar fi: procesoare de texte, calcule tabelare, e-mail; managementul bazelor de date; interacțiunea cu aplicațiile web; grafică; prelucrări vocale; proiectare etc.

Calculatoare de mână *(handheld computers)*, cum ar fi asistenții digitali personali (*PDA - Personal Digital Assistants*), constituie cea mai portabilă soluție, acestea fiind dispozitive ușoare care însă sunt mai puțin performante decât sistemele laptop, dar mult mai potrivite pentru aplicații în care cerințele sunt limitate. Dispozitivele PDA sunt referite ca *handhelds*, *palmtops*, *PDAs*, *Palm Pilots*, *Palms* și *iPAQs*. Posibilitățile de introducere a datelor sunt reduse, dar există soluții specifice, precum scrisul direct pe ecranul acestuia, combinat cu pachete software de recunoaștere a scrisului de mână. PDA-urile sunt dispozitivele ideale pentru *managementul calendarului și al activităților normale de business*, cu ajutorul cărora se pot efectua operații de vizualizare și editare a contactelor, întâlnirilor și a notelor scurte. În același timp, textele foarte lungi nu pot fi introduse ușor cu tastatura unui astfel de dispozitiv și, chiar dacă s-ar încerca, este posibil ca dimensiunea documentului în cauză să depășească capacitatea de stocare a dispozitivului. Un PDA este foarte ușor de folosit pentru operațiile simple, acestea putând fi efectuate în timp redus, cu toate că un laptop poate oferi aceleași servicii, dar este mult mai incomod de folosit de un agent mobil. PDA-urile au capacitatea de a realiza o interfață cu PC-urile pentru *backup* sau transferul informațiilor importante. De asemenea, informația de pe un PC poate fi descărcată pe un PDA, pe care rulează variante reduse ale sistemelor de operare și software clasic instalat.

Telefoanele mobile creează un compromis între puterea și funcționalitatea laptop-urilor și portabilitatea PDA-urilor; oferă majoritatea opțiunilor disponible pe un PDA. Telefoanele mobile sunt din ce în ce mai mult utilizate în servicii de tip banking.

Minicalculatorul este cunoscut ca un calculator de mărime medie, ce nu este portabil. El suportă până la 50 de utilizatori simultan și are o memorie principală de capacitate mare. În mod normal, minicalculatorul deservește o rețea de terminale simple. Minicalculatoare pot fi utilizate ca servere de rețea și ca servere în internet.

Calculatorul mainframe reprezintă un calculator de mari dimensiuni și foarte puternic care este amplasat într-un cadru care poate fi controlat. Un astfel de calculator suportă prelucrări cerute de sute, chiar mii de utilizatori, precum și calcule specializate. Calculatoarele mainframe sunt folosite în organizațiile de mari dimensiuni, unde datele și programele partajate sunt accesate de un număr mare de utilizatori. Mainframe urile sunt folosite ca servere pentru afaceri electronice/tranzacții.

Supercalculatorul posedă resurse hardware şi software deosebite, fiind cele mai puternice calculatoare; sunt utilizate în rezolvarea unor probleme care necesită calcule complexe. Supercalculatoarele sunt utilizate în industria de apărare, în câteva universităţi, în agenţii guvernamentale, în domeniul afacerilor, în cercetarea ştiinţifică din domeniul industriei aeronautice şi spaţiale.

O condiţie importantă pentru buna funcţionare a SI este întreţinerea corespunzătoare a echipamentelor hardware, care trebuie specificată într-un program dedicat acestei activităţi. Auditorul SI trebuie să verifice dacă acest program a fost aprobat de conducerea companiei şi în ce măsură costurile de întreţinere depăşesc bugetul prevăzut sau sunt foarte ridicate.

Există mai multe proceduri de monitorizare a utilizării calculatorului, dintre care cele mai importante sunt:

- **raportul de disponibilitate** al sistemului (**availability**), care măsoară timpul în care sistemul este operaţional pentru a fi utilizat. Indicatorul opus acestuia este **downtime**, care reprezintă timpul în care sistemul nu este operaţional. Dacă acest indicator este mare, rezultă că facilităţile hardware sunt inadecvate, întreţinerea sistemului de operare ocupă mult timp sau o pregătire necorespunzătoare a operatorilor;
- **raportul privind erorile hardware**, care înregistrează toate disfuncţionalităţile pe UCP, echipamentele periferice şi căderile de tensiune. Acest raport este revizuit periodic de managerul SI pentru a întreprinde măsurile de corecţie ce se impun;
- **raportul de utilizare** pentru UCP şi echipamentele periferice, care este folosit de managerul SI în planificarea şi alocarea resurselor informaţionale.

4.3. Operarea SI

Operarea SI este o activitate care caracterizează în principal sistemele informaţionale centralizate, în care introducerea datelor, prelucrarea acestora şi obţinerea rezultatelor se realizează în mod regulat şi cu o frecvenţă prestabilită.

4.3.1. Managementul operării SI

Managementul operării SI include trei funcţii principale:

- stabilirea standardelor şi procedurilor de operare SI în deplină concordanţă cu strategia şi politicile entităţii;
- asigurarea resurselor necesare pentru operarea SI;
- monitorizarea operării SI, măsurarea performanţelor în acest domeniu şi perfecţionarea acestora.

Îndeplinirea acestor funcţii presupune un set de controale, dintre care amintim:

- controlul planificării în timp, la nivel de detaliu, a lucrărilor ce urmează să fie executate;
- autorizarea și monitorizarea utilizării resurselor informaționale în concordanță cu politicile entității;
- monitorizarea conformității operării SI cu standardele prestabilite;
- detectarea încercărilor de operare frauduloasă în cadrul SI și rezolvarea problemelor de securitate care apar într-un timp rezonabil;
- autorizarea și controlul modificărilor în programarea lucrărilor ce urmează să fie executate;
- controlul jurnalului de operare și identificarea neconcordanțelor dintre lucrările planificate și cele executate;
- întreținerea rapoartelor de contabilitate a lucrărilor și a înregistrărilor de credit;
- limitarea accesului fizic la resursele de calcul a personalului, în funcție de cerințele de operare.

Managementul serviciilor IT este un concept mai larg, care cuprinde procesele și procedurile privind suportul și funcțiile oferite de serviciile IT în mod eficient, eficace și în concordanță cu strategia de dezvoltare a entității.

Suportul serviciilor IT cuprinde: biroul serviciului, managementul incidentelor, managementul configurării și managementul schimbării. Serviciile IT oferite cuprind: managementul serviciului, managementul financiar, managementul capacității, managementul continuității și disponibilității acestora. Fiecare dintre procesele enumerate înainte sunt de sine stătatoare, dar, în același timp, pe un plan superior sunt interdependente unele de altele.

Instrumentul de lucru utilizat pentru un management eficient al serviciilor IT este **Service Level Agreement (SLA)**, care definește tipul serviciului, structura și funcțiile, timpul de utilizare și alte informații relevante. Acest instrument este absolut necesar în cazul externalizării. Spre exemplu, dacă un incident apare de mai multe ori, acesta devine o problemă, care va implica unele modificări majore sub controlul managementului schimbării și al configurării.

Orice serviciu IT trebuie să satisfacă cerințele utilizatorilor finali. Pentru a monitoriza calitatea, eficiența și eficacitatea serviciilor IT, există mai multe instrumente dintre care cele mai importante sunt:

- **raportul joburilor terminate anormal**, care include informații relevante privind condițiile de terminare. Dacă numărul de joburi terminate anormal este mare, atunci rezultă că: proiectarea, realizarea și testarea SI s-au făcut superficial, instrucțiunile și suportul de operare sunt inadecvate sau personalul de operare este slab pregătit. Terminarea anormală a unei lucrări se datorează mai multor tipuri de erori, care au surse diverse: programul utilizatorului, sistemul de operare, operatorul, rețeaua, liniile de

telecomunicaţii, componenta hardware. Uneori, furnizorii de echipamente hardware intervin direct în configurarea acestora, trecând peste măsurile de securitate fără ca beneficiarii să ştie acest lucru. Această procedură trebuie bine controlată pentru că reprezintă o metodă de acces neautorizat, care poate produce pagube;

- **raportul privind problemele apărute în timpul operării SI** trebuie revăzut de conducerea compartimentului de operare pentru a verifica dacă acţiunile întreprinse de operatori în asemenea situaţii au fost corecte sau nu;
- **raportul de distribuţie a rezultatelor exploatării SI**;
- **jurnalul de operare** include informaţii complete privind principalele activităţi întreprinse de sistemul de operare şi operatorul uman pe parcursul execuţiei lucrărilor. Acesta este un document foarte important, care poate fi folosit de auditor pentru a verifica dacă:
    - numai programele aprobate pentru execuţie, conform planificării, au fost efectiv executate;
    - programele utilitare ale sistemului de operare care vizează modificarea datelor şi a programelor SI au fost folosite numai pentru scopurile prevăzute;
    - fişierele de date prevăzute a fi parolate au fost protejate;
    - accesul programelor la datele sensibile este aprobat.

4.3.2. Operarea infrastructurii IT

Operarea infrastructurii IT se face prin proceduri automate sau manuale şi implică atât componenta hardware, cât şi pe cea software. Există două categorii principale de operatori:

- **de sistem**, care asigură operarea execuţiei lucrărilor planificate având în general tangenţă cu sistemul de operare şi programele utilitare ale acestuia;
- **de introducere date**, care asigură actualizarea permanentă a bazelor de date folosite de diverse SI.

Operatorii de sistem trebuie să îndeplinească următoarele sarcini: execuţia lucrărilor, restartarea lucrărilor terminate anormal după ce au fost întreprinse corecţiile necesare, salvarea periodică a fişierelor de lucru în copii de siguranţă (*backup files*), monitorizează accesul autorizat la facilităţile de calcul, monitorizează execuţia lucrărilor în concordanţă cu procedurile de planificare a acestora, monitorizează performanţele şi disponibilitatea resurselor informaţionale, participă la testarea procesului de recuperare în caz de dezastre. Aceste servicii sunt detaliate în proceduri de operare hardware, software şi ale fiecărui SI.

Odată cu evoluţia în domeniul IT, introducerea centralizată a datelor printr-un serviciu specializat acestui scop a fost înlocuită de aplicaţii on-line interactive de

colectare a datelor. Această schimbare a condus la introducerea unor controale noi privind:
- separarea sarcinilor de introducere a datelor de cele de validare a acestora;
- înregistrarea unor informații suplimentare privind introducerea datelor cum ar fi: data, ora și identificarea persoanei;
- chei de verificare suplimentară.

În majoritatea sistemelor de operare moderne există două instrumente care ajută și oferă informații relevante pentru managementul operării SI:
- contabilitatea automată a lucrărilor (*job accounting*), care furnizează informații privind timpul de utilizare a echipamentelor periferice, pentru fiecare lucrare, informații care pot fi folosite pentru analiza performanțelor hardware în vederea optimizării acestora;
- planificatorul automat al lucrărilor, care reduce posibilitățile de eroare și crește performanța de utilizare a sistemului de calcul.

Pe parcursul exploatării SI, apar o serie de incidente, cu diferite grade de dificultate, care trebuie analizate cu multă atenție și rezolvate în timp util. Acestea sunt semnalate în general de utilizatorii sistemului, și pentru rezolvarea lor este necesară intervenția specialiștilor care au creat sistemele respective. Întreținerea sistemelor informaționale este o problemă tot așa de importantă ca și realizarea acestora. Prin urmare, după testarea finală a sistemului și darea în exploatare, este necesară crearea unui **suport tehnic** format dintr-o interfață între utilizatori și sistem (*help desk*), managementul SI și administratorul sistemului, care urmărește mentenanța acestuia.

În categoria programelor de serviciu intră și **programele utilitare**, care pot fi împărțite din punct de vedere funcțional în cinci categorii:
- înțelegerea și documentarea SI: diagrama fluxului (*flowcharter*), analizorul profilului tranzacției (*transaction profile analyzer*), analizorul execuției (*executive path analyzer*) și dicționarul datelor (*data dictionary*);
- evaluarea și testarea calității datelor: utilitare de manipulare a datelor (*data manipulation utilities*), vidarea și listarea memoriei principale (*dump/lister*), utilitar pentru compararea datelor (*data comparison utility*) și facilități de interogare (*query facility*);
- testarea funcționării programelor și a integrității datelor: generatorul datelor de test (*test data generator*), facilități de depanare on-line (*online debugging facility*), analizor al ieșirilor (*output analyzer*) și simulator de rețea (*network simulator*);
- asistarea dezvoltării rapide a programelor: utilitar de afișare vizuală (*visual display utility*), copierea bibliotecii (*library copy*), editor de texte (*text editor*), facilități de codificare on-line (*online coding facility*), generator de rapoarte (*report generator*) și generatoare de coduri (*code generators*);

- creşterea eficienţei operaţionale: monitoare pentru utilizarea CPU şi a memoriei, precum şi analizoare pentru liniile de comunicaţie.

O problemă foarte importantă în utilizarea software-ului este licenţierea acestuia. Pentru a preveni şi detecta utilizarea fără licenţă a software-ului, auditorul SI trebuie să:
- verifice politicile şi procedurile de protecţie împotriva utilizării neautorizate a software-ului. Unele companii cer angajaţilor lor să semneze o declaraţie privind respectarea acestor proceduri;
- verifice concordanţa dintre licenţele acordate şi utilizarea efectivă a acestora.

Există câteva posibilităţi care pot fi folosite pentru a preveni utilizarea software-ului fără licenţă:
- centralizarea controlului privind distribuţia şi instalarea software-ului;
- inhibarea unităţilor de floppy disc şi accesul aplicaţiilor dintr-o reţea locală protejată;
- instalarea unui program de control al licenţelor pe reţeaua locală şi accesul staţiilor de lucru la software-ul de aplicaţii prin intermediul acestui program, care poate depista eventualele încercări de apelare frauduloasă;
- scanarea periodică a staţiilor de lucru pentru a verifica dacă s-au încărcat copii neautorizate.

Un alt control foarte puternic împotriva utilizării fără licenţă a software-ului într-o reţea de calculatoare este **licenţa de site** (*site licensing agreement*), care permite accesul unui număr de utilizatori la reţea. Există, de asemenea, o **licenţă concurentă** (*concurrent license agreement*), care permite unui număr de utilizatori să acceseze simultan un anumit software.

4.4. Arhitectura software a SI

În funcţie de rolul pe care îl joacă în cadrul unui sistem de calcul, software-ul se împarte în două categorii: software de sistem şi software de aplicaţii.

4.4.1. Software de sistem

Software de sistem (sistemul de operare) este un ansamblu de programe care reprezintă primul nivel de interfaţă între utilizator şi componenta hardware. El este compus din două categorii de programe: de comandă-control şi de serviciu.

Programele de comandă-control, cunoscute sub numele de *supervizor, monitor, executiv*, constituie nucleul sistemului de operare. Ele se încarcă de pe disc în memoria principală într-o zonă protejată, la momentul iniţializării sistemului şi rămân acolo până la oprirea acestuia. Principalele funcţii pe care le îndeplinesc aceste programe sunt următoarele: tratarea întreruperilor hardware, alocarea şi eliberarea

memoriei principale și auxiliare pentru execuția lucrărilor utilizatorilor, lansarea în execuție a lucrărilor utilizatorilor, sincronizarea și comunicarea între lucrările aflate în execuție, lansarea operațiilor de intrare/ieșire.

Programele de serviciu, spre deosebire de cele de comandă-control, se încarcă de pe disc în memoria principală în funcție de cerințele de prelucrare la momente diferite și rămân în memoria principală numai pe perioada execuției acestora. Din această categorie fac parte: compilatoarele, translatoarele, editoarele de legături, programele utilitare, programele de planificare a lucrărilor utilizator.

Majoritatea sistemelor de operare sunt realizate asfel încât să răspundă tuturor cerințelor utilizatorilor, indiferent de mărimea și complexitatea aplicațiilor pe care aceștia le exploatează. Altfel spus, un sistem de operare este un pachet de programe generalizat și parametrizat, care, pentru a fi folosit la nivelul unei companii, trebuie adaptat cerințelor specifice ale acesteia. Asfel, utilizând kitul de instalare, printr-o procedură de generare, utilizând o serie de parametri, se croiește un sistem de operare potrivit unei anumite entități. Principalii parametri de control după care se generează un sistem de operare vizează: gestiunea datelor și a resurselor informaționale, stabilirea priorităților de lucru și managementul lucrărilor. Din punct de vedere al auditorului SI, este foarte important să se evalueze modul de configurare a parametrilor de control ai sistemului de operare, care ar putea conduce la coruperea datelor, nedetectarea unor erori, accesul neautorizat la resursele informaționale etc.

Având în vedere rolul important pe care îl are sistemul de operare într-un sitem de calcul, integritatea acestuia reprezintă un factor important, care trebuie întreținută prin mecanisme care să permită:

- protecția împotriva unor modificări neautorizate;
- execuția programelor utilizator nu trebuie să interfereze cu cele ale sistemului de operare;
- izolarea proceselor în timpul execuției acestora pentru a se asigura că:
  - ✓ mai multe procese care se execută simultan în zone de memorie separate nu pot accesa date dintr-o zonă care nu le aparține;
  - ✓ procesele se execută numai în concordanță cu prioritățile stabilite diferențiat pentru fiecare în parte, iar aceste priorități nu pot fi modificate accidental.

Din aceste motive, prin componenta hardware se asigură două moduri de lucru pentru orice sistem de calcul: **stare supervizor** și stare **program utilizator**. În starea de lucru supervizor lucrează numai nucleul sistemului de operare (programele de comandă-control), care au acces nelimitat la toate resursele sistemului. De aceea se spune că starea supervizor este o **stare privilegiată**. Celelalte programe ale sistemului de operare, precum și programele utilizatorilor operează în modul de lucru program utilizator, care este un **mod neprivilegiat**. Un utilizator care lucrează în modul neprivilegiat și reușește în mod fraudulos, exploatând o vulnerabilitate a sistemului de

operare să ajungă în modul de lucru privilegiat poate produce mari pagube în sistem. Iată de ce o configurare necorespunzătoare a sistemului de operare reprezintă un mare risc în exploatarea sistemului.

Pentru procesul de auditare a SI, sunt foarte importante jurnalele de urmărire a diverselor activităţi în care este implicat sistemul de operare, cum ar fi:

- accesul programelor la datele senzitive;
- programele planificate şi executate;
- versiunile fişierelor utilizate în procesul de prelucrare;
- operarea componentelor care asigură integritatea sistemului de operare;
- securitatea accesului la bazele de date;
- validarea documentaţiei privind administrarea bazelor de date;
- conformitatea cu standardele organizaţiei.

4.4.2. Software de aplicaţii

Software-ul de aplicaţii oferă instrumentele necesare pentru dezvoltarea aplicaţiilor utilizator, din această categorie făcând parte: instrumentele de birotică (Word, Excel, Power Point), sistemele de gestiune a bazelor de date (SGBD), generatoare de sisteme expert etc. Aceste programe au acelaşi regim ca şi programele de serviciu, fiind încărcate de pe disc în memoria principală pentru execuţie, în funcţie de necesităţi.

Sistemele de operare moderne includ facilităţi noi privind alocarea şi utilizarea optimă a resurselor, cum ar fi conceptul de **memorie virtuală**, a cărei capacitate este dată de capacitatea memoriei principale plus capacitatea memoriei auxiliare instalate la momentul considerat. Acest concept de memorie virtuală operează cu: spaţiul virtual de adresă, spaţiu fizic de adresă şi o funcţie de translatare a unei adrese virtuale într-o adresă fizică reală. Memoria virtuală este organizată la nivel de: pagină, segment şi segment-pagină, implicând o migraţie a informaţiei în ambele sensuri între memoria principală şi memoria auxiliară pe baza unor algoritmi specifici.

Un alt concept introdus de sistemele de operare actuale este acela de **firmware,** care reprezintă o parte din software realizat cu ajutorul unor microprograme în memorii de tip ROM. Acest concept creşte viteza de execuţie a sistemului de operare.

4.4.3. Tipuri de sisteme de operare

După 1980, odată cu apariţia primelor reţele de calculatoare, au început să se folosească *sistemele de operare în reţea* sau *sistemele de operare distribuite*, ca o completare a *sistemelor de operare centralizate* (care mai sunt cunoscute ca sisteme de operare monoprocesor).

După modul în care utilizatorii și programele acestora au acces la sistemul de calcul, sistemele de operare pot fi clasificate în:

- **multiutilizator (*timesharing*)**, care permit mai multor utilizatori să folosească sistemul și să execute programele în mod simultan. Sistemele de operare incluse în această categorie sunt: *UNIX, Windows 2000, Windows 3.1x, Windows 95, Windows 98, Windows NT*;
- **multiprocesare,** care utilizează mai multe procesoare dar partajează aceeași memorie principală pentru a executa simultan mai multe programe. Din această categorie fac parte: *UNIX, Windows 2000, Windows NT 4.0*;
- **multitasking**, care permit ca mai multe procese să fie încărcate în același timp și executate concurent;
- **multithreading,** care permit diferitelor părți ale programelor să fie executate concurențial. Sistemele de operare incluse în această categorie sunt: *UNIX, Windows 2000, Windows 95, Windows 98, Windows NT 4.0.*

4.5. Gestiunea datelor

Organizarea datelor din punct de vedere informatic are două componente:

- organizarea datelor în memoria internă a calculatorului, care cuprinde structurile de tip: listă, coadă și stivă;
- organizarea datelor pe memoria externă, care cuprinde structurile de tip fișier și bază de date.

Un fișier este un ansamblu de înregistrări fizice, omogene din punct de vedere al conținutului și al prelucrării. O *înregistrare fizică* este unitatea de transfer între memoria internă și cea externă a calculatorului. Aceasta este formată din una sau mai multe înregistrări logice. O *înregistrare logică* este unitatea de prelucrare din punct de vedere al programului-utilizator. Aceasta este formată dintr-un ansamblu de *câmpuri*, care descriu o anumită realitate.

Există trei metode de organizare a datelor în fișiere:

- **secvențială** – prin care căutarea unei înregistrări se face prin parcurgerea tuturor înregistrărilor precedente;
- **indexat-secvențială** – potrivit căreia accesul la o înregisrare se face pe baza valorii unei chei, care face parte din înregistrare, și căutarea secvențială a acesteia într-o tabelă de indecși;
- **directă**, prin care accesul la o înregistrare se face pe baza unei chei, care nu face parte din înregistrare, fiind generată aleatoriu.

O *bază de date* poate fi definită ca un ansamblu de date elementare sau structurate, accesibile unei comunități de utilizatori. Mai concret, o bază de date, este un

ansamblu de fişiere intercorelate, care conţine date necesare unui sistem informatic (aplicaţie informatică).

4.5.1. Sistemul de gestiune a bazelor de date

Sistemul de gestiune a bazelor de date (SGBD) constituie o interfaţă între utilizatori şi baza de date (BD), care permite în principal crearea, actualizarea şi consultarea acesteia. În acest context putem defini SGBD–ul ca un instrument de asamblare, codificare, aranjare, protecţie şi regăsire a datelor în BD. Principalele obiective ale SGBD-ului sunt:

- independenţa datelor faţă de programele de aplicaţii;
- manipularea datelor prin limbaje declarative (neprocedurale);
- prelucrarea eficientă a tranzacţiilor asupa BD;
- posibilitatea accesului direct la date;
- posibilitatea maximizării consistenţei datelor;
- minimizarea costului de întreţinere a BD prin partajarea datelor;
- reducerea redundanţei;
- întărirea securităţii datelor.

Independenţa datelor faţă de programele de aplicaţii a condus la o abstractizare a datelor pe trei niveluri de reprezentare (scheme): *extern, conceptual şi intern.*

Independenţa fizică a datelor

Schema internă a BD descrie modul în care datele sunt organizate pe suportul fizic (fişiere, înregistrări), precum şi metodele de acces, criteriile de ordonare şi regăsire a acestora, astfel încât să se asigure un grad de performanţă şi supleţe cât mai ridicat. Independenţa fizică a datelor constă în posibilitatea de a schimba organizarea internă a datelor şi structurile de înregistrare, fără a modifica programele care le folosesc (programe-utilizator). Raportându-ne la structura pe cele trei niveluri, aceasta înseamnă independenţa schemei interne de cea conceptuală.

Independenţa logică a datelor

Schema conceptuală a BD se obţine printr-o sinteză şi integrare a schemelor externe, care reprezintă interese informaţionale de grup sau individuale ale utilizatorilor. În aceste condiţii, este normal ca fiecare grup de utilizatori să aibă posibilitatea să-şi modifice în timp cerinţele informaţionale fără a afecta schema conceptuală a BD.

Independenţa logică a datelor constă în posibilitatea de a modifica schemele externe fără a modifica schema conceptuală. Principalele avantaje ale independenţei logice a datelor sunt următoarele:

- permite oricărui grup de utilizatori să vizualizeze datele aşa cum îşi doresc;

- permite evoluția în timp a schemelor externe ale fiecărui grup de utilizatori fără a afecta schema conceptuală;
- permite evoluția unei anumite scheme externe fără a afecta celelalte scheme externe.

Metadatele sunt date care descriu elementele unei BD. Corespunzător celor trei scheme de reprezentare (externă, conceptuală și internă), există trei tipuri de metadate. Dicționarul datelor (DD) și directorul sistem (DS) definesc și memorează în format sursă și obiect toate definițiile pentru cele trei scheme, precum și transformările asociate acestora (*mappings*). Astfel, DD conține un index și o descriere pentru fiecare câmp al BD, iar DS înregistrează adresa fizică de pe disc și metoda de acces aferente fiecărui câmp.

Există cinci tipuri de modele privind structurarea datelor în BD: ierarhic, rețea, relațional, obiect și relațional-obiect. Modelul ierarhic presupune utilizarea unei structuri arborescente, în care fiecare element-fiu este subordonat unui singur element-părinte, care la rândul lui poate avea mai mulți fii. Modelul rețea se bazează pe principiul că un element-fiu poate fi subordonat la mai multe elemente-părinte, generând o pânză de păianjen. În majoritatea BD actuale se folosesc modelele relațional și obiect.

4.5.2. Modelul relațional de strucurare a datelor în BD

Modelul relațional a fost introdus de E.F. Codd în 1970 și are la bază conceptul de *relație* definit în teoria matematică a mulțimilor ca fiind o submulțime a produsului cartezian al mai multor mulțimi: $R \subseteq M_1 \times M_2 \times \ldots \times M_n$. Familia de mulțimi pe care este definită relația se numește *domeniu*, iar dacă $M_1 = M_2 = \ldots = M_n$, relația este omogenă. Numărul n se numește *gradul* relației, un element al relației $t = (m_1, m_2, \ldots, -m_n)$ este numit *tuplu*, iar numărul de tupluri indică *cardinalitatea* relației.

Schema unei relații este formată din numele relației, atributele acesteia și restricțiile de integritate. **Domeniul** reprezintă mulțimea tuturor valorilor posibile care definesc o anumită proprietate a unui obiect, spre deosebire de atribut, care reprezintă mulțimea valorilor **existente** la un moment dat în coloana pe care o desemnează în cadrul relației. Într-o relație pot exista mai multe atribute care iau valori în aceleași domenii.

Relațiile se reprezintă într-o formă simplă prin tabele, supuse următoarelor restricții:
- în fiecare coloană toate valorile sunt de același fel;
- fiecare valoare este reprezentată printr-un număr sau un șir de caractere (nu trebuie să fie grup sau ansamblu);
- ordinea liniilor în tabel nu este predefinită și nu sunt admise duplicate;

- coloanele sunt identificate prin nume distincte care reprezintă atributele relaţiei.

Tuplurile unei relaţii se pot identifica în mod unic prin intermediul valorilor unuia sau mai multor atribute (eventual toate atributele), care joacă rol de **cheie primară** a relaţiei respective. Se numeşte **cheie externă** a unei relaţii un atribut care este cheie primară într-o altă relaţie. Legăturile dintre cheile externe şi cheile primare corespondente constituie un element fundamental în utilizarea modelului relaţional (figura 4.5.1).

Deoarece relaţiile reflectă un anumit aspect din realitate, acestea se supun unor restricţii care sunt de două tipuri:

- **restricţii de integritate** care depind de semantica valorilor domeniilor şi care cer ca relaţiile să se supună următoarelor reguli:
  - ✓ *integritatea entităţii*, prin care valorile cheii primare trebuie să fie unice şi nenule;
  - ✓ *integritatea referirii*, potrivit căreia valorile unei chei externe trebuie să refere valorile cheii primare corespondente.
- **alte restricţii** care se aplică asupra domeniilor, reflectând anumite corelaţii de ordin valoric (egalitate, inegalitate).

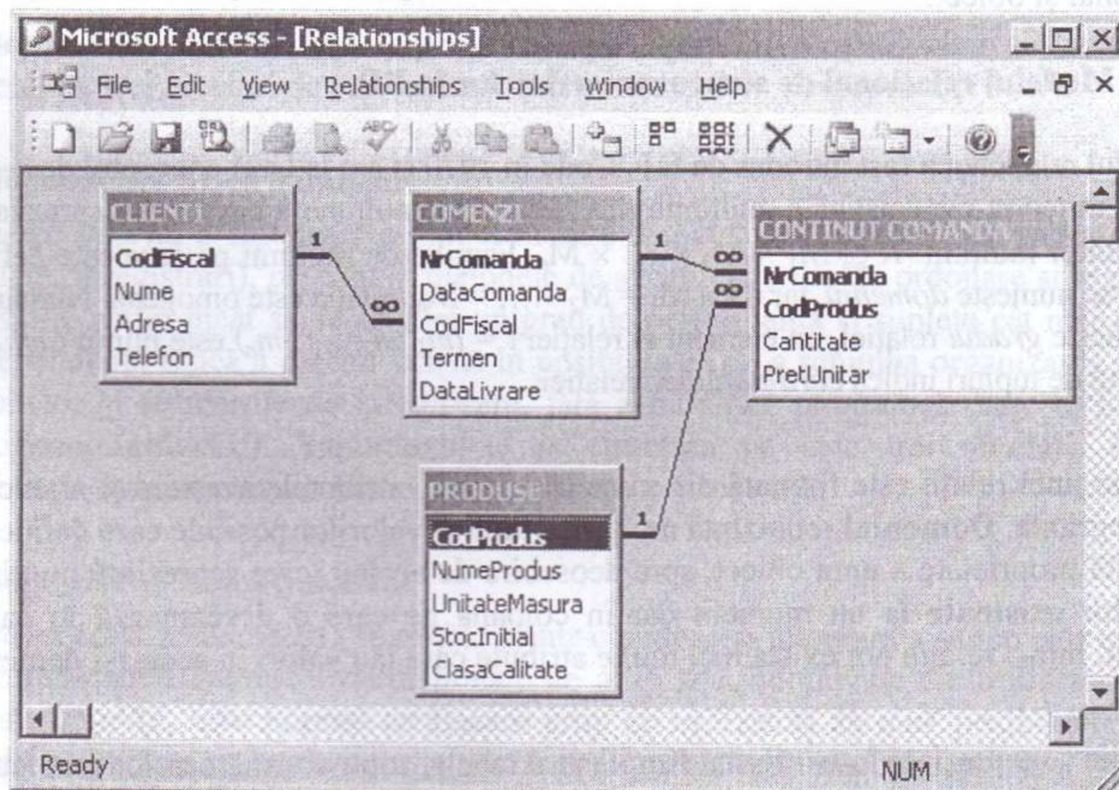


Figura 4.5.1. **Implementarea în SGBD Access a modelului relaţional**

Normalizarea relaţiilor

E.F. Codd a arătat că într-o anumită formă relaţiile posedă proprietăţi nedorite, pe care le-a numit **anomalii de actualizare** (*adăugare, ştergere, modificare*). Pentru a înlătura aceste anomalii, Codd a stabilit trei forme normale pentru relaţii şi a introdus procesul de normalizare care se bazează pe noţiunea de **dependenţă funcţională (FD)** ca relaţie între atributele unei entităţi ce are un caracter invariant. O relaţie este în *forma normală 1 (1NF)*, dacă şi numai dacă toate atributele ei conţin numai valori atomice. O relaţie este în *forma normală 2 (2NF)* dacă şi numai dacă este în 1NF şi orice atribut noncheie este complet dependent funcţional de cheia primară. O relaţie este în *forma normală 3 (3NF)* dacă şi numai dacă este în 2NF şi fiecare atribut noncheie nu este dependent tranzitiv pe cheia primară.

4.5.3. Controalele BD

Integritatea şi disponibilitatea BD sunt asigurate prin intermediul următoarelor controale:

- definirea standard a câmpurilor BD prin dicţionarul datelor;
- implementarea procedurilor de salvare (*backup*) şi recuperare (*recovery*) care asigură disponibilitatea BD;
- controale de acces la nivel de câmpuri, tabele şi fişiere pentru a preveni accesul neautorizat;
- controale privind modificarea BD numai de către persoane autorizate;
- controale privind rezolvarea accesului concurent la date de către mai mulţi utilizatori simultan (blocarea înregistrărilor pe perioada tranzacţiei);
- controale privind completitudinea, consistenţa şi relaţiile dintre elementele BD, care sunt implementate la nivelul definirii structurii BD, ceea ce nu permite violarea acestora prin programele de exploatare a BD sau utilitarele SGBD-ului;
- utilizarea unor puncte de verificare şi refacere a relaţiilor dintre elementele BD;
- utilizarea unor proceduri de restructurare a BD atunci când au loc modificări la nivel conceptual, logic sau fizic;
- utilizarea instrumentelor de măsurare a performanţelor BD pentru monitorizarea şi menţinerea eficienţei acesteia.

4.6. Infrastructura de reţea a SI

Reţeaua de calculatoare este un ansamblu de sisteme de calcul interconectate prin intermediul unor medii de comunicaţie (cablu coaxial, fibră optică, linie telefonică, unde radio), care permite folosirea în comun, de către mai mulţi utilizatori, a resurselor fizice (hardware), logice (software de bază şi aplicaţii) şi informaţionale (fişiere, baze de date), asociate calculatoarelor din reţea.

4.6.1. Tipuri de reţele de calculatoare

După aria geografică de răspândire, există trei tipuri de reţele de calculatoare:
Reţele **PAN** (*Personal Area Network*) şi **WPAN** (*Wireless PAN*) reprezintă toate dispozitivele informatice interconectate într-un spaţiu de ordinul metrilor: calculatoare personale, mouse, cameră web, tastatură, imprimantă.

Reţele **LAN** *(Local Area Network)* şi **WLAN** *(Wireless LAN)* - sunt în general reţele private localizate într-o singură clădire sau într-un campus de cel mult câţiva kilometri şi care oferă servicii informaţionale în interiorul unei companii (trasfer de fişiere, partajarea imprimantelor şi a discurilor, e-mail). Au viteze mari de comunicare a datelor (10 Mbps, 100 Mbps, 1 Gbps, 10 Gbps), sunt uşor de instalat şi administrat, prezintă o securitate redusă a datelor, iar mediul de comunicaţie poate fi cablu coaxial, fibră optică sau unde radio.

Reţele **WAN** *(Wide Area Network)* şi **WWAN** *(Wireless WAN)* (figura 4.6.1) – sunt reţele pe arii întinse, care interconectează subreţelele locale ale unei organizaţii care sunt dispersate geografic la nivel naţional sau internaţional pentru a oferi servicii de comunicare (transfer de fişiere, e-mail, conectare la distanţă, chat, videoconferinţă, administrare la distanţă).

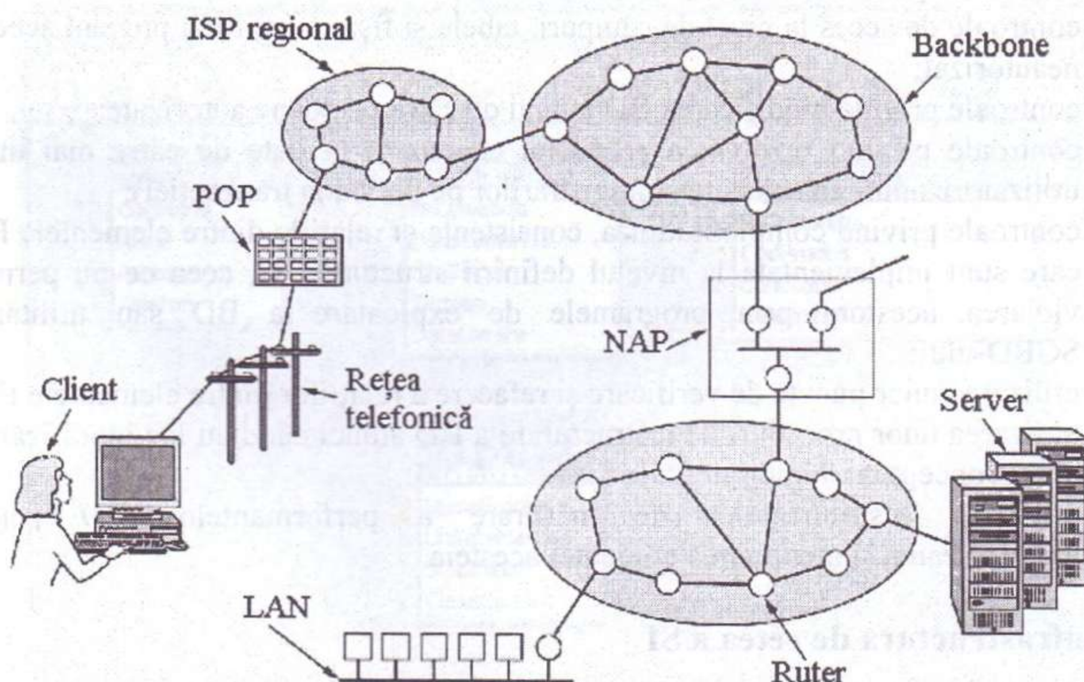


Figura 4.6.1. **Reţea WAN**

POP: Point of Presence
NAP: Network Access Point
ISP: Internet Access Provider

Principalele caracteristici ale acestor reţele sunt: viteze mici de comunicaţie (56 kbps, 64 kbps, 128 kbps, 1544 Mbps, 2048 Mbps), lucrează în general după arhitectura client-server, protecţia datelor este greu de realizat împotriva accesului neautorizat. Comunicarea se face prin infrastructura deja creată pentru telefonie, prin satelit, dar şi prin infrastructură proprie (cum ar fi liniile de fibră optică pe sub ocean care leagă două continente).

Reţele **MAN** *(Metropolitan Area Network)* şi **WMAN** *(Wireless MAN)* reprezintă o extensie a reţelelor LAN şi utilizează în mod normal tehnologii similare cu acestea. Aceste reţele pot fi atât private, cât şi publice.

Reţele **SAN** *(Storage Area Networks)* reprezintă un tip particular de reţele LAN, dedicate interconectării dispozitivelor de memorare pentru a centraliza memorarea şi administrarea datelor unei companii.

O altă clasificare a reţelelor se poate face luând în considerare modul în care se asigură comunicaţia între diferitele noduri ale reţelei, adică după **tipul subreţelei de comunicaţie**. Reţeaua în care fiecare nod utilizator poate comunica la cerere cu oricare altul poartă numele de **reţea cu comutare**. Există două tipuri de comutare: **comutarea de circuite** şi **comutarea logică** (*store and forward*).

Prin comutarea de circuite se stabileşte un canal între două noduri ale reţelei, care este fizic rezervat şi disponibil pe întreaga durată a comunicaţiei. Comutarea logică poate fi: **comutare de mesaje** şi **comutare de pachete**. Prin comutarea de mesaje, fiecare mesaj este transmis de la un nod la altul în întregime, ca o entitate unică. Acest mod de comutare nu poate asigura administrarea optimă a resurselor şi ca urmare a fost înlocuit prin comutarea de pachete.

Tehnica de comutare prin pachete apelează la fragmentarea mesajelor în unităţi de mărime mai mică (pachete), fiecare conţinând propria adresă, ca şi informaţia necesară pentru rutare.

În opoziţie cu reţelele cu comutare, există reţelele fără comutare, în care nodurile sunt interconectate prin canale **specializate**. Astfel, o cale **dedicată** poate lega două noduri, permiţând o transmisie **punct-la-punct.**

4.6.2. Standarde şi protocoale de reţea

Standardele şi protocoalele pentru reţele trebuie să răspundă la patru cerinţe principale: **interoperabilitatea** (posibilitatea de conectare a unor echipamente cu structuri hardware şi proceduri de operare diverse), **disponibilitatea** (oferă serviciu de calitate şapte zile pe sătămână, 24 de ore pe zi), **flexibilitate** (permit extinderea

rapidă a reţelei atât din punct de vedere al componentei hardware cât şi al aplicaţiilor) şi **întreţinerea** (suport de întreţinere integrat pentru toate echipamentele din reţea).

Modelul de referinţă OSI/ISO

Pentru a evita multiplicarea soluţiilor de interconectare a sistemelor care au la bază arhitecturi eterogene, **ISO** (*International Standards Organization*) a dezvoltat **modelul de referinţă OSI** (*Open System Interconection*) prezentat în figura 4.6.2 Acest model permite interconectarea sistemelor de origini diferite, dar care respectă reguli standard. Regulile sunt formalizate prin protocoale. Protocoalele se referă la modul în care trebuie să se efectueze comunicaţiile. Sistemele care sunt conforme cu aceste convenţii sunt numite **sisteme deschise**.

Modelul de referinţă OSI nu se referă la arhitectura internă a sistemelor, ci la comportamentul lor extern, care permite comunicaţia. Unul dintre elementele esenţiale, în concepţia modelului de referinţă OSI, a constat în stabilirea unei frontiere clare între două domenii de funcţii: transmisia informaţiilor, care cuprinde nivelurile de bază 1 la 4 şi prelucrarea acestora, care se realizează prin nivelurile 5 la 7. Serviciile nivelului transport au acest rol de interfaţă.

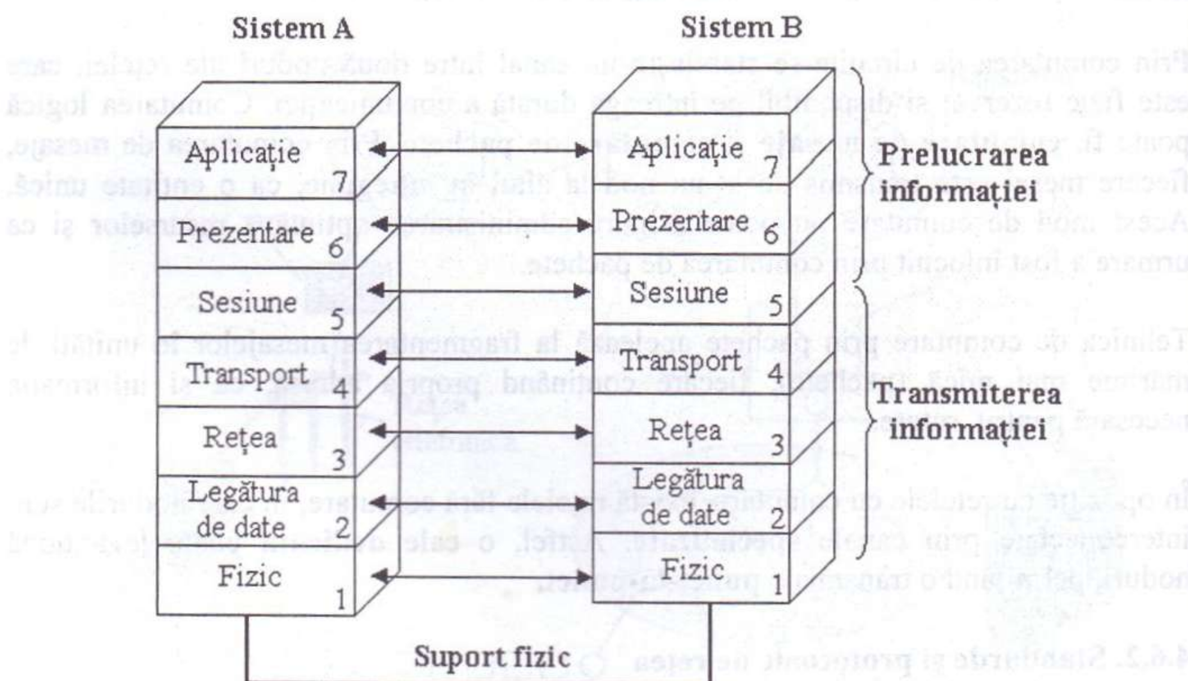


Figura 4.6.2 **Modelul de referinţă OSI**

Nivelul fizic realizează funcţiile legate de gestiunea şi exploatarea suporturilor fizice de comunicaţie (cablu, conectori, carduri): interfeţe mecanice şi electrice, proceduri de recepţie şi emisie a informaţiei binare (serializare/deserializare, codificare

/decodificare), adaptarea semnalelor la suport (modulare/demodulare). La acest nivel, cu unele mici excepţii, nu se detectează şi nu se corectează erorile de transmisie.

Nivelul legătură de date primeşte pachetele de date de pe nivelul reţea, le transformă în cadre şi le transmite sub forma unor şiruri de biţi nivelului fizic. Principalele funcţii realizate la acest nivel sunt:

- sincronizarea emiţătorului şi receptorului prin utilizarea unor indicatoare (*flags*);
- controlul fluxului de date, pentru a limita debitul emitorului la cel al receptorului;
- detectarea şi recuperarea erorilor între două puncte ale legăturii de date.

Detectarea şi corectarea erorilor se fac prin utilizarea metodei CRC (*Cyclic Redundancy Check*), potrivit căreia în momentul emiterii unui mesaj, utilizând şirul de biţi asociat acestuia, pe baza unui algoritm prestabilit, se calculează o valoare CRC. La recepţie, utilizând şirul de biţi recepţionat, pe baza aceluiaşi algoritm, se recalculează CRC-ul şi se compară cu cel transmis; dacă sunt egale nu există eroare, în caz contrar sunt erori de transmisie care urmează să fie corectate.

Nivelul reţea creează un circuit virtual între emiţător şi receptor, care permite rutarea şi transmiterea mai departe a pachetelor, tratarea erorilor şi a controlul congestiilor. Tot aici sunt pregătite pachetele pentru nivelul legăturii de date prin conversia acestora în unul sau mai multe *datagram* şi se determină adresa MAC (*Media Access Control*) pentru următoarea destinaţie, care poate fi un ruter. Poate asigura multiplexarea mai multor comunicaţii pe aceeaşi legătură de date.

Nivelul transport asigură transferul datelor în condiţii de siguranţă şi transparenţă între emiţător şi receptor, recuperarea erorilor şi controlul fluxului. Acest nivel verifică confirmarea recepţiei integrale a fiecărui pachet de date, în caz contrar retransmite pachetul.

Nivelul sesiune controlează dialogul dintre emiţător şi receptor. Acesta stabileşte, controlează şi termină conexiunea dintre emiţător şi receptor. Toate conversaţiile, schimburile de date şi dialogul dintre nivelurile aplicaţie sunt controlate de nivelul sesiune.

Nivelul prezentare transformă datele pentru a furniza o interfaţă standard spre nivelul aplicaţie şi realizează unele funcţii cum ar fi codificarea datelor, compresia textului şi reformatarea. Acest nivel converteşte datele de ieşire într-un format acceptat de standardul de reţea şi le transferă nivelului sesiune. Similar, converteşte datele recepţionate din nivelul sesiune într-un format acceptat de nivelul aplicaţie.

Nivelul aplicaţie oferă o interfaţă standard pentru aplicaţiile care trebuie să comunice cu dispozitivele din reţea (imprimarea în reţea, e-mail, memorarea datelor pe un file server) şi nu trebuie confundat cu software-ul de aplicaţii.

4.6.3. Reţele locale de calculatoare (*LAN – Local Area Network*)

Din punct de vedere al standardului OSI/ISO, reţelele locale se bazează pe comutarea de pachete, costul transmisiei depinzând de dimensiunea şi numărul pachetelor, şi nu de destinaţia la care acestea sunt transmise.

Există trei modalităţi de transmisie a pachetelor într-o reţea LAN:

- unicast – pachetul este transmis de la un emiţător la un singur receptor;
- multicast – pachetul este transmis la mai multe noduri din reţea în funcţie de un anumit criteriu;
- broadcast – pachetul este transmis la toate nodurile reţelei.

Din punct de vedere al suportului fizic de comunicaţie există şase posibilităţi: cablu torsadat, cablu coaxial, fibră optică, unde radio, microunde radio şi sateliţi.

Cablul torsadat este format din două conductoare de cupru, izolate unul de celălalt şi înfăşurat în mod elicoidal de-a lungul axei longitudinale. Acesta se foloseşte pentru distanţe mici (până la 60 de metri), este uşor de instalat şi modificat şi suportă transmisii de date şi voce. Este sensibil la interferenţele electromagnetice, care produc erori de transmisie.

Cablul coaxial are o capacitate mai mare şi este mai scump decât cablul torsadat, putând transporta simultan date şi semnale video. Poate fi folosit pentru distanţe mai mari (între 100 şi 800 de metri) decât cablul torsadat şi este rezistent la interferenţele electromagnetice.

Fibra optică este folosită pentru distanţe mari şi suportă transmisii de date, voce, imagini şi video. Nu radiază energie şi este un bun conductor electric, nu este influenţată de interferenţele electromagnetice. Este scumpă şi se poate folosi pentru transmisii de bandă largă. **Undele radio** se folosesc pentru transmisii de date pe distanţe mici. Sunt sensibile la interferenţele electromagnetice. **Microundele radio** se folosesc pentru transmisii de date şi voce, sunt sensibile la interferenţele electromagnetice şi sunt afectate de condiţiile atmosferice şi obiectele solide.

Sateliţii de telecomunicaţii folosesc transmiţător/receptor (*transponder*) care primeşte un semnal de la o staţie terestră şi îl retransmite pe altă frecvenţă altor staţii terestre. Lucrează în bandă largă cu frecvenţe diferite şi pot transporta volume mari de date. Sunt sensibili la interferenţele electromagnetice şi la condiţiile atmosferice. Au un mare dezavantaj comparativ cu ceilalţi suporţi tehnici, şi anume întârzierea în transmisie din cauza distanţei până la satelit.

Pentru accesul la suportul fizic de comunicaţie există două tehnologii: **Ethernet** (*Standardul IEEE 802.3*) şi **Token Ring** (*Standardul IEEE 802.5*).

Tehnologia **Ethernet** a început cu viteza de 10 Mbps și a ajuns astăzi la 100 Mbps (*Fast Ethernet)* și 1 Gbps *(Gigabit Ethernet)*. În timpul transmisiei prin tehnologia Ethernet apar următoarele evenimente:

- fiecare colaborator din rețea ascultă traficul pe suportul fizic de comunicație;
- un calculator (stație) transmite numai dacă suportul de comunicație este liber;
- dacă două stații încearcă să ocupe suportul de comunicație simultan apare o coliziune;
- dacă apare o coliziune, transmisia este întreruptă și se reia după un interval de timp.

Tehnologia **Token Ring** se utilizează într-o rețea cu topologie inel. Un cadru particular, numit token circulă în permanență prin inel și poate fi ocupat sau liber. Fiecare stație ascultă suportul de comunicație și dacă prinde un token liber îl ocupă și transmite un pachet de date către o altă stație. Stația de destinație ascultă suportul de comunicație și când găsește un token, care transportă un pachet pentru acesta, îl recepționează și eliberează token-ul. În felul acesta, spre deosebire de tehnologia Ethernet, sunt excluse coliziunile. Utilizarea fibrei optice ca suport de comunicație pentru tehnologia token ring permite extinderea rețelelor locale până la o distanță de 2 km.

4.6.4. Topologia rețelelor locale de calculatoare

Topologia rețelelor LAN definește modul de organizare logică a rețelei și modalitatea de conectare a stațiilor de lucru (nodurile). Există patru topologii pentru rețelele LAN: magistrală (*bus*), inel (*ring*), stea (*star*) și plasă (*mesh*).
În **topologia magistrală** stațiile de lucru sunt conectate de-a lungul unei magistrale de comunicație, care este ușor de asamblat și utilizat. Se poate extinde ușor prin utilizarea unor repetoare. Dezavantajul acestei topologii constă în faptul că o întrerupere a magistralei sau funcționarea defectuoasă a unei stații afectează întreaga rețea.

În **topologia inel** stațiile de lucru sunt conectate la un mediu de comunicație configurat într-un inel. Această topologie se folosește în rețelele care utilizează tehnologia token ring sau fibră optică (*FDDI – Fiber Distributed Data Interface*) și are performanțe ridicate în rețelele cu un număr unic de stații sau în rețelele cu un număr mare de stații, dar cu o încărcare uniformă a acestora. Comparativ cu alte topologii, acoperă distanțe mari și poate fi extinsă ușor. Dezavantajele acestei topologii constau în faptul că este dificil de instalat, este scumpă, iar nefuncționarea unei stații blochează întreaga rețea. Pentru a preveni o asemenea situație de blocaj al rețelei, se folosesc o serie de facilități cum sunt monitorizarea activă (*active monitoring*), selectarea stațiilor cu probleme și izolarea acestora de restul rețelei și apoi activarea rețelei rămase. Astfel, când apare o problemă în rețea, se generează un cadru care circulă pe la toate stațiile și culege informații referitoare la incident. În final aceste informații sunt folosite de o stație care le interpretează pentru a reconfigura rețeaua și a elimina problemele apărute.

În **topologia stea** staţiile de lucru sunt conectate prin cabluri separate la un hub sau *switch* central, care le interconectează între ele. Avantajele acestei topologii constau în faptul că este uşor de adăugat sau scos o staţie din reţea, o staţie defectă nu întrerupe întreaga reţea, iar diagnoza reţelei se face prin hub-ul sau switch-ul central. Dezavantajul acestei topologii constă în faptul că dacă apar probleme în hub-ul central şi nu există un altul de rezervă (care să-l înlocuiască automat), cade întreaga reţea.

În **topologia plasă** orice staţie poate fi conectată cu oricare alta. Avantajele acestei topologii constau în faptul că problemele din reţea sunt uşor de diagnosticat, iar în situaţia în care o staţie cade, traficul este redirecţionat printr-un alt nod. Dezavantajele constau în costuri ridicate de instalare şi întreţinere.

Principalele criterii folosite pentru alegerea tehnologiei LAN sunt: *modul de transfer*, *lungimea de bandă pentru transmisie*, *bugetul alocat* şi *tipul de management de la distanţă*. Spre exemplu, dacă avem o aplicaţie care necesită transfer de date, semnale audio şi video, se poate folosi modul de transmisie asincron (*Asynchronous Transfer Mode – ATM*), care necesită un *switch* de nivel 2 în cadrul modelului OSI. Lungimea de bandă este dependentă de traficul din reţea, care depinde de comunicarea dintre servere şi staţiile de lucru. Bugetul alocat este dependent de introducerea noilor tehnologii (*hub*-uri inteligente, *switch*-uri de nivel 3 şi 4), care sunt foarte scumpe. Managementul de la distanţă al reţelei se face prin intermediul unor agenţi incluşi în hub-uri şi switch-uri, care permit captarea protocoalelor şi filtrarea mesajelor la toate nivelurile modelului OSI.

4.6.5. Echipamente de reţea

Repetorul (*repeater*) lucreză pe nivelul fizic şi permite extinderea unei reţele LAN sau conectarea a două segmente separate de reţea, care folosesc aceeaşi tehnologie (*Ethernet* sau *Token Ring*), dar care pot avea medii de transmisie diferite. El primeşte semnalele dintr-un segment de reţea, le amplifică (regenerează) pentru a compensa atenuările din timpul transmisiei şi apoi le trimite către celălalt segment de reţea. Un dezavantaj al repetorului este acela că el copiază semnalul electronic, inclusiv zgomotul, de la un segment de reţea la altul.

Hub-ul lucrează la nivel fizic şi poate fi considerat ca un repetor cu mai multe porturi. Dacă în mod obişnuit un repetor are două porturi, un hub poate avea de la patru la douăzeci şi patru de ieşiri. Utilizarea unui hub duce la schimbarea topologiei unei reţele de la reţea de tip magistrală (*bus*), unde fiecare dispozitiv este direct conectat pe linia principală, la o topologie de tip stea. În cazul huburilor, datele provenite de pe un port sunt transmise pe toate celelalte segmente ale reţelei, excepţie făcând portul prin care datele au fost transmise. Huburile pot fi împărţite în trei

categorii: *pasive* – care servesc doar ca o conexiune fizică pentru punerea în comun a unui mediu fizic, *active* – care amplifică semnalul primit înainte de a-l transmite mai departe către celelalte porturi şi *hub*-uri *inteligente* – care funcţionează în linii mari ca şi huburile active, dar au în dotare un microprocesor şi capacităţi de diagnosticare. Uneori hub-urile poartă denumirea de *concentratoare*, deoarece servesc ca o conexiune centrală pentru o reţea locală de tip Ethernet.

Puntea (*bridge*) lucrează la nivelul legăturii de date şi funcţionează pe principiul că fiecare nod de reţea are propria adresă fizică (*Media Access Control - MAC*). Puntea permite interconectarea reţelelor LAN de acelaşi tip sau de tipuri diferite sau poate crea două segmente separate de reţele LAN sau WAN dintr-un singur segment, pentru a reduce coliziunile. Puntea utilizează o tabelă de rutare pentru a memora informaţiile despre adresele calculatoarelor unde se transferă datele. Cele două segmente lucrează ca două reţele LAN diferite înainte de nivelul legăturii de date, dar după acest nivel, mai sus, ele devin din punct de vedere logic o singură reţea. Puntea memorează pachetele recepţionate şi le retransmite spre destinaţiile acestora. Deoarece sunt dispozitive care se bazează în principal pe proceduri software, nu sunt aşa de performante ca cele bazate pe hardware, cum sunt switch-urile şi prin urmare sunt mai puţin folosite. Dacă într-o firmă există mai multe reţele cu topologii diferite, atunci administrarea fluxurilor de date poate fi făcută de un calculator echipat cu mai multe plăci de reţea, care va juca rolul de punte între aceste reţele, el asociind reţelele fizice diferite într-o singură reţea logică. Spre deosebire de repetor, puntea este capabilă să decodeze cadrul pe care-l primeşte pentru a face prelucrările necesare transmiterii pe reţeaua vecină.

Switch-ul de nivel 2 (legătura de date) poate separa sau interconecta segmentele unei reţele LAN de tip Ethernet pentru a reduce coliziunile. Acestea memorează cadrele recepţionate, filtrează şi retransmit pachetele între segmentele reţelei ca şi *hub*-urile sau *bridge*-urile, dar utilizând protocoale specializate care sunt implementate prin circuite hardware. Un *switch* este uneori descris ca o punte cu mai multe porturi. *Switch*-ul nu transmite datele către toate porturile aşa cum face hub-ul. De aceea, traficul prin reţea scade datorită filtrării pachetelor. Decizia de filtrare este simplă, switch-ul citind adresa de destinaţie înainte de a selecta portul. Segmentarea duce la împărţirea reţelei în domenii de coliziune, transferul de date între segmente făcându-se pe cât posibil simultan. Switch-urile, ca şi hub-urile suportă linii redundante de comunicaţie. Dacă una dintre legături cade, cealaltă este folosită, acest lucru făcându-se transparent pentru utilizator.

Ruterul (*router*) funcţionează la nivelul reţea al modelului ISO/OSI şi este utilizat pentru interconectarea mai multor reţele locale de tipuri diferite, dar care utilizează acelaşi protocol de nivel fizic. Utilizarea lor asigură o mai mare flexibilitate a reţelei în ceea ce priveşte topologia acesteia. La fel ca şi la punte, informaţiile sunt memorate în tabele de rutare, care conţin adrese de reţea. Diferenţa între o punte şi un

ruter este că în timp ce puntea operează cu adresele fizice ale calculatoarelor (MAC), ruterele utilizează adresele logice ale acestora. În timp ce o punte interconectează mai multe reţele fizice diferite într-o singură reţea logică, un ruter interconectează reţele logice diferite. Aceste adrese logice sunt administrate de nivelul reţea şi nu depind de tipul reţelei locale. O caracteristică este aceea că ruterele nu pot comunica direct cu calculatoarele aflate la distanţă, din această cauză ele nu verifică adresa sistemului destinaţie, ci doar adresa reţelei de destinaţie.

Ruterul ia decizii privitoare la traseul pe care urmează să-l parcurgă pachetul pentru a ajunge la destinaţie. Datorită capacităţii de a determina cel mai bun traseu, printr-o serie de legături de date, de la o reţea locală în care se află sistemul sursă la reţeaua locală în care se află sistemul destinaţie, un sistem de rutere poate asigura mai multe trasee active între cele două reţele, făcând posibilă transmiterea mesajelor de la sistemul sursă la sistemul destinaţie pe căi diferite.

Switch-ul de nivel 3 şi 4 (reţea şi transport) reprezintă ultimele noutăţi în materie de *switch*-uri. Acestea recepţionează pachetele, extrag adresele IP de destinaţie, le compară cu adresele din tabela de adrese şi determină cea mai bună cale pentru a ajunge la destinaţie. Se creează astfel un circuit virtual între sursă şi destinaţie pentru determinarea *domeniului de difuzare a mesajelor* (*broadcast domain*), care reprezintă un segment de reţea în care toate staţiile din acesta pot fi simultan accesate utilizând aceeaşi adresă, numită *adresa de difuzare*.

Brouterul este un echipament care combină calităţile unei punţi şi ale unui router, putând acţiona ca ruter pentru un anumit protocol si ca punte pentru altele. Acesta poate fi folosit pentru a conecta două reţele locale, care utilizează protocoale la nivelul legăturilor de date diferite prin furnizarea unor funcţii ale routerului.

Porţile (*gateway*) de acces fac posibilă comunicaţia între sisteme cu arhitecturi diferite şi medii incompatibile. În general, aceste echipamente permit conectarea la un mainframe al reţelelor locale. Ele realizează o conversie de protocol pentru toate cele şapte niveluri OSI.

4.6.6. Reţele pe arii întinse *(WAN – Wide Area Network)*

Reţelele de tip WAN interconectează reţele de tip LAN pe arii geografice extinse, la nivel de oraş, ţară şi mondial. Principalele caracteristici ale acestor reţele sunt următoarele: lucrează pe linii comutate sau dedicate, în modul simplex, semiduplex sau duplex, utilizând primele trei niveluri din modelul OSI (fizic, legătură de date şi reţea).

Principalele tehnici de transmisie utilizate de aceste reţele sunt:

- **comutarea de mesaje** constă în transmiterea unui mesaj complet la un punct central de memorare şi retransmiterea acestuia la punctul de destinaţie atunci când calea de comunicaţie devine disponibilă. Costul transmisiei depinde de lungimea mesajului;
- **comutarea de pachete** constă în spargerea mesajului în unităţi mai mici numite pachete şi transmiterea lor individuală prin reţea în funcţie de disponibilitatea canalului de comunicaţie. Costul transmisiei se calculează pe pachet şi nu depinde de distanţa şi traseul până la destinaţie;
- **comutarea de circuite** constă în stabilirea unui canal direct de comunicaţie între sursă şi destinaţie prin comutarea circuitelor reţelei. Odată stabilit acest canal, este utilizat exclusiv de sursă şi destinaţie. Această reţea poate fi de tip punct la punct, (linii închiriate), multipunct, reţeaua de telefonie publică sau o reţea digitală de servicii integrate (*Integrated Services Digital Network – ISDN*);
- **circuitul virtual,** care se stabileşte între cele două echipamente din reţea pentru a permite un transfer în siguranţă al datelor. Aceste circuite sunt de două feluri: circuit virtual comutat şi permanent;
- **WAN dial-up service** utilizând conectarea sincronă sau asincronă pentru organizaţiile care au un mare număr de utilizatori mobili. Lungimea de bandă în acest caz este mică, iar performanţele sunt scăzute.

Deoarece reţelele LAN sunt incluse în reţele WAN, putem spune că echipamentele folosite în reţelele LAN se regăsesc în cele de tip WAN. În plus, un echipament foarte des folosit în reţelele WAN este **modemul** (modulator/demodulator) care converteşte semnalele digitale, care vin din calculator în semnale analogice, pentru a fi transmise pe liniile telefonice, precum şi operaţia inversă de conversie din semnale analogice în semnale digitale. Pentru realizarea acestor operaţii, modemul foloseşte două metode de transmisie:

- **sincronă**, în care biţii sunt transmişi fără întrerupere cu o viteză constantă, iar modemul emite un caracter de sincronizare la începutul transmisiei unui bloc de date;
- **asincronă**, în care fiecare byte este precedat de un bit de start şi urmat de un bit de stop. Această metodă este simplă, dar nu este eficientă.

Un loc important în cadrul reţelelor WAN îl ocupă reţelele private virtuale (*Virtual Private Networks – VPN*), care asigură o securitate sporită prin codificarea pachetelor de mesaje şi transmiterea acestora prin conexiuni virtuale utilizând infrastructura internet. Există trei tipuri de reţele VPN: VPN cu acces de la distanţă (*remote access VPN*) folosite pentru conectarea utilizatorilor mobili la reţeaua WAN a companiei, *Intranet VPN*, care conectează birourile la reţeaua WAN a întreprinderii, şi *Extranet VPN*, care oferă partenerilor de afaceri un acces limitat la fiecare reţea a altor companii.

4.6.7. Reţele fără fir (*Wireless*)

Pentru reducerea costurilor de comunicaţie şi a creşterii productivităţii, majoritatea organizaţiilor apelează la reţelele fără fir. Oamenii de afaceri, persoanele din management, dar şi numeroase alte categorii de angajaţi au nevoie de date indiferent de locul unde se află ei fizic, şi se aşteaptă ca accesul la acestea să fie rapid şi uşor de configurat. Aceste lucruri pot fi asigurate de dezvoltarea tehnologiilor reţelelor wireless, care, pe lângă comoditatea utilizării dispozitivelor fără a fi îngrădiţi de o conexiune fizică, oferă şi o securitate din ce în ce mai bună şi de asemenea viteze de transfer al datelor din ce în ce mai mari.

Tehnologiile wireless, la modul cel mai simplu, pot fi definite ca modalitatea de realizare a comunicării între două sau mai multe dispozitive fără a fi efectuate conexiuni fizice între dispozitivele respective. În acest scop sunt utilizate diferite frecvenţe radio, care sunt reglementate de comitete de standardizare astfel încât diferite dispozitive realizate de diferiţi producători să poată comunica fără probleme. Pentru anumite frecvenţe trebuie achiziţionate licenţe de la autorităţile din fiecare ţară, iar alte frecvenţe, cum ar fi cea de 2,4 GHz, sunt libere, deci nu trebuie realizată nicio notificare către organismele de reglementare, oricine poate folosi gratuit dispozitive care emit şi recepţionează în această bandă de frecvenţă.

Reţelele wireless pot fi clasificate în mai multe tipuri, în funcţie de complexitate, puterea de emisie, frecvenţa utilizată, raza de acoperire etc. În funcţie de complexitate, reţelele pot fi *Wireless Wide Area Networks* (*WWAN*) sau *Wireless Local Area Networks* (*WLAN*), cum sunt de exemplu reţelele de telefonie mobilă ce folosesc „celule" pentru acoperirea unor suprafeţe de foarte mari dimensiuni sau de mai mică complexitate, cum ar fi diversele dispozitive pentru acasă sau firme mici: microfoane, căşti, camere web, mouse şi tastaturi fără fir, incluzând aici şi dispozitivele *bluetooth* sau *IR* (*Infrared*).

Creşterea gradului de utilizare a acestor reţele necesită tratarea diverselor probleme ce pot apărea din punct de vedere al securităţii datelor transmise. Dacă într-o reţea datele circulă prin intermediul cablurilor de date, este mult mai uşor de asigurat o monitorizare a dispozitivelor conectate şi a punctelor de acces în reţea. Asigurarea securităţii şi monitorizarea reţelei devine mult mai dificilă într-o reţea de tip wireless, unde mediul de transmisie a datelor este realizat de frecvenţele radio, iar acestea se propagă în mod normal pe o suprafaţă circulară de mai multe sute de metri în jurul punctului de transmisie. Oriunde în interiorul acestei suprafeţe circulare pot fi aşezate dispozitive care, fiind în raza de acţiune a emiţătorului, pot compromite securitatea reţelei în cazul în care nu se face o autentificare eficientă a dispozitivelor.

O altă problemă care poate apărea în cazul rețelelor wireless este faptul că unele aplicații ar trebui actualizate astfel încât să poată funcționa prin intermediul rețelelor fără fir. Deși de cele mai multe ori mediul de transmisie – prin cablu sau prin frecvențe radio – este transparent pentru beneficiarii rețelelor de comunicații, există și unele aplicații speciale pentru care trebuie făcute modificări în vederea utilizării lor eficiente.

Avantajele majore pentru utilizatorii rețelelor wireless (LAN) sunt flexibilitatea și mobilitatea pe care le au aceștia. Ei se pot deplasa fără nicio problemă în întreaga arie de acoperire a rețelei cu tot cu laptopurile sau PDA-urile lor, arie care de cele mai multe ori este de 100 m în interiorul clădirilor sau de 300 m în exterior. Aria de acoperire poate fi foarte ușor mărită sau combinată cu ajutorulor repetitoarelor sau prin combinația între rețele cu fir și rețele fără fir.

4.6.8. Rețeaua internet

Internetul este o rețea de rețele, la scară mondială, care oferă servicii on-line și nu este controlată de nimeni. Mai multe rețele regionale se interconectează între ele și apoi prin intermediul unui punct de acces (*Netwok Access Point – NAP*) se conectează la o magistrală (*backbone*) de mare viteză la care sunt conectate și alte rețele regionale. Ne putem imagina prin similitudine rețeaua internet ca și rețeaua de autostrăzi, drumuri naționale, drumuri județene și locale, care comunică unele cu altele. Conectarea între două rețele pe Internet se face prin intermediul unui ruter. Fiecare calculator conectat la internet se numește host și are o adresă IP, care este furnizată de Autoritatea Națională de Alocare a Adreselor Internet. La nivel mondial, există o autoritate, care gestionează adresele și care le distribuie la autoritățile locale, care mai departe le alocă diverșilor utilizatori (companii sau persoane fizice). Conectarea la internet se poate face în două moduri: *direct* sau prin intermediul unui *furnizor de servicii* (*Internet Service Provider – IPS*).

Internetul folosește un sistem de protocoale numit TCP/IP (*Transmition Control Protocol/Internet Protocol*), care este un standard *de facto* echivalent cu standardul OSI (figura 4.6.3).

Cel mai utilizat serviciu internet este World Wide Web (www), care se bazează pe conceptul de hipertext și folosește modelul client-server. Potrivit acestui model, pe un calculator server, utilizând limbajele HTML (*HyperText Markup Language*) sau XML (*Extended Markup Language*) se creează resursele web (documente, informații), care pot fi accesate de la distanță, de un calculator (client) prin intermediul unui program numit navigator sau browser (Internet Explorer, Mozilla Firefox).

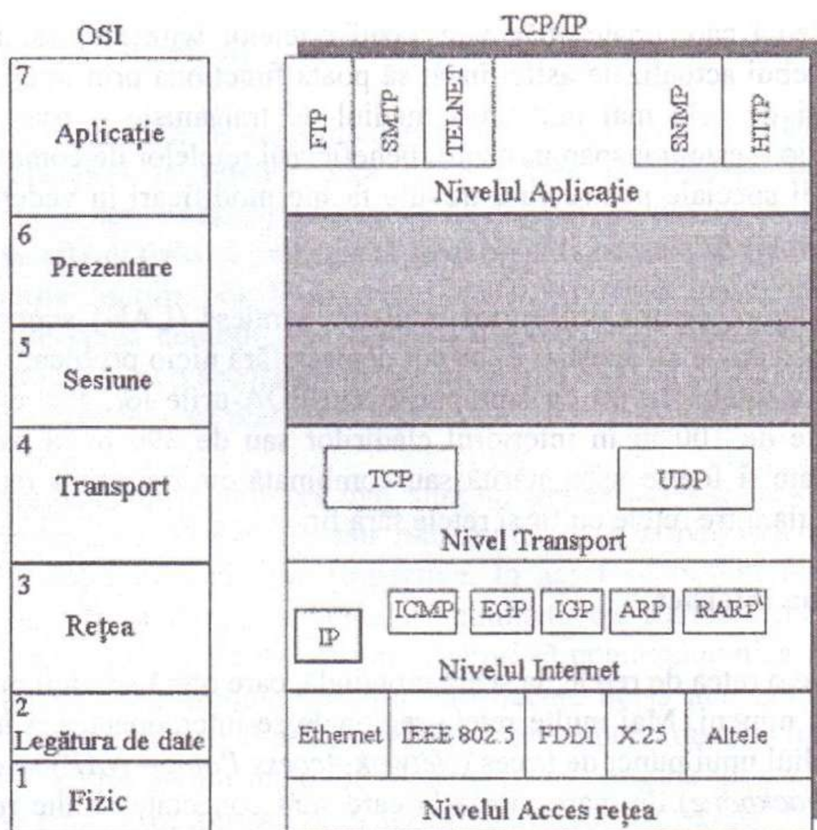


Figura 4.6.3 **Arhitectura TCP/IP**

Principalele concepte legate de serviciul web sunt:

- **URL** (*Universal Resource Locator*) – permite identificarea unei resurse pe internet. Sintaxa unui URL este:
  `protocol://nume_server/cale/nume_document`,
  unde `protocol` poate fi: *HTTP* (*HiperText Transfer Protocol*), *ftp* (*file transfer protocol*), *telnet* (acces la distanţă) sau *mailto*;
- **CGI** (*Common Gateway Interface*) – un program care se execută pe server în scopul prelucrării datelor dintr-un formular web transmis de un client;
- **Cookie** – un mesaj reţinut de browser-ul web pentru identificarea utilizatorilor în scopul pregătirii unor pagini specifice pentru aceştia;
- **Applet** – un program în limbajul Java încărcat de pe server pe calculatorul client pentru a fi executat local în scopul realizării unei funcţii (crearea unui formular web, validarea unor date de intrare, execuţia unui program audio/video). Execuţia applet-urilor presupune un anumit risc pentru calculatorul clientului (pe care se execută) în ceea ce priveşte scurgerea unor informaţii confidenţiale. De aceea, anumite browsere sunt configurate astfel încât să nu permită execuţia applet-urilor, decât după autorizarea din partea utilizatorului;

- **Servlet** – este un applet Java sau un program care se execută pe server similar unui CGI, diferența constă în faptul că servlet-ul rămâne în memoria internă și poate deservi mai multe cereri din partea clienților;
- **DNS** (*Domain Name Service*) este un sistem care convertește numele *host*-urilor în adrese IP și invers;
- **Remote Terminal Control Protocol** permite accesul de la distanță la un calculator conectat la internet;
- **Conectare directă** – o rețea de tip LAN este conectată la internet, ceea ce înseamnă că toate calculatoarele din rețeaua respectivă au acces complet și permanent la internet;
- **Internet appliance** – un dispozitiv de dimensiuni mici, cum ar fi PDA (*Personal Digital Assistant*) sau un telefon mobil, care are încorporate funcții web;
- **FTP** permite schimbul de fișiere pe internet;
- **SMTP** (*Simple Mail Transport Protocol*) protocolul pentru poșta electronică;
- **Transborder data flow** se referă la transferul datelor între două țări prin internet, ceea ce implică măsuri de securitate specifice.

4.6.9. Administrarea rețelelor

Administrarea rețelelor se face prin intermediul instrumentelor specifice, care în general sunt incluse în sistemul de operare al rețelei și sunt folosite de administratorul de rețea. Principalele funcții ale unui sistem de operare în rețea sunt: accesul local sau de la distanță la servere și host-uri, partajarea resurselor rețelei (fișiere, componente, spațiul de memorare), legătura dintre host-uri și servere, documentarea on-line privind utilizarea rețelei.

Există doi indicatori care pot măsura performanțele unei rețele:

- **timpul de așteptare** (*latency*) este timpul necesar unui semnal pentru a ajunge dintr-un punct al rețelei în altul. Într-o rețea TCP/IP acest indicator se măsoară cu ajutorul comenzii *ping*;
- **capacitatea de transfer** (*thronghput*) măsoară numărul de bytes transmiși pe secundă.

Principalele activități privind managementul rețelelor de calculatoare sunt:

- managementul incidentelor (*fault management*) – depistarea dispozitivelor defecte din rețea;
- managementul configurării (*configuration management*) permite utilizatorilor definirea și schimbarea de la distanță a configurației oricărui dispozitiv din rețea;
- contabilitatea utilizării resurselor rețelei;
- managementul performanței rețelei;
- managementul securității rețelei.

Instrumentele care permit managementul reţelei sunt:

- **timpul de răspuns** (*response time reports*) măsoară intervalul de timp dintre introducerea unei comenzi şi răspunsul dat de sistem;
- **timpul de cădere a sistemului** (*downtime reports*) este timpul de nefuncţionare ca urmare a diverselor cauze (întreruperea energiei electrice, erori de operare, trafic mare). Dacă acest timp este mare, atunci se impun măsuri corective;
- **monitorul on-line** controlează corectitudinea transmisiilor de date prin verificarea ecoului transmisiei;
- **analizorul de protocol** (*protocol analyzer*) este un instrument de diagnostic, care lucrează la nivelul legăturii de date sau reţea din modelul OSI. Acesta furnizează următoarele informaţii: protocolul utilizat, tipul de pachete transmise, analiza traficului, erorile;
- **SNMP** (*Simple Nerwork Management Protocol*) controlează şi monitorizează diferite variabile din reţea, furnizează statistici privind performanţele şi securitatea reţelei. Informaţiile obţinute pot fi afişate pe o consolă principală, dar sistemul este capabil să primească din partea operatorului comenzi privind starea oricărui dispozitiv din reţea (ruter, switch). Pentru a răspunde acestor solicitări, fiecare dispozitiv implicat în cerere trebuie să aibă un agent SNMP.

Majoritatea aplicaţiilor din reţea se bazează pe arhitectura *client-server*, potrivit căreia două programe care rulează pe două calculatoare diferite (server şi client) depind mutual unul de celălalt pentru a distribui un serviciu în reţea. Această arhitectură se poate implementa în două moduri:

- pe două niveluri: un calculator server (bază de date sau *back-end*) şi un client, care include un program de acces la server;
- pe trei niveluri: un client (mai puţin dotat), care accesează prin intermediul unei interfeţe serviciul agent, un grup de unul sau mai multe *servere* de aplicaţii şi un grup de unul sau mai multe servere de baze de date.

Un termen foarte des folosit în aplicaţiile *client-server* este cel de *middleware*, care se interpune între aplicaţii şi reţeaua de calculatoare şi gestionează interacţiunea dintre client şi server. Acesta facilitează conexiunea client-server şi permite aplicaţiei client să acceseze şi modifice baza de date aflată la distanţă pe un server sau fişierele unui mainframe.

4.7. Auditul infrastructurii tehnice SI

Schimbarea permanentă a tehnologiei infrastructurii şi a tipului de operare a dus la diversificarea modului de auditare şi analizelor specifice pentru: hardware, sisteme de operare, baze de date, reţele de calculatoare, controale ale operării în reţea, operarea SI, operaţii de ieşire, raportarea problemelor de gestionare, raportarea privind

disponibilitatea şi utilizarea hardware, precum şi planificarea acestora. Pentru fiecare dintre acestea vor fi urmărite proceduri de analiză.

Tabelul 4.7.1. **Analiza hardware**

Nr. crt.	Tipul analizei	Conţinut	Evaluare
1.	Proceduri de gestionare hardware	Asigurarea analizei continue a hardware-ului şi performanţa software-ului utilizat pe aceste platforme	Proceduri de evaluare a performanţei hardware
		Criterii utilizate în planul de monitorizare a performanţei hardware	Date şi analize istorice obţinute din rapoarte, log-uri, planificări ale proceselor, planificări de prevenire şi întreţinere
2.	Plan pentru achiziţii controlate de hardware	Planul de achiziţii este sincronizat cu planul de afaceri al societăţii	Se poate identifica mai uşor lipsa unui echipament
		Planul conţine specificaţii tehnologice ale echipamentelor existente	Se poate face o alegere a echipamentelor noi mai potrivită cu necesităţile societăţii
		Concordanţa între documentaţie şi specificaţiile hardware şi software	Cererea şi achiziţionarea de echipamente hardware se fac conform cerinţelor software
3.	Criterii de achiziţionare a PC-urilor	Cererile de achiziţie a calculatoarelor se bazează pe analiza cost-beneficiu (profit)	Se vor avea în vedere avantajele reducerilor de preţ sau alte beneficii calitative sau cantitative
4.	Controale pentru înlocuirea echipamentelor hardware existente	Schimbările de echipamente hardware sunt comunicate inginerului de sistem	Sunt făcute teste de lucru pe noile echipamente pentru aplicaţiile şi bazele de date existente

Tabelul 4.7.2. **Analiza sistemului de operare**

Nr. crt.	Tipul analizei	Conţinut	Evaluare
1.	Intervievarea personalului serviciului tehnic	Proceduri-test pentru software-ul implementat	Cerinţe din documentaţie
2.	Proceduri de selecţie a software-ului	Cerinţe de control şi procesare a SI, limitele software-ului	Cerinţele SI în concordanţă cu afacerea
3.	Studiu de fezabilitate şi procese de selecţie	Obiectivele sistemului se bazează pe cerere/ofertă	Criteriile de selecţie sunt aplicate la toate elementele din ofertă
4.	Analiza cost-beneficiu a procedurilor sistemului	Costurile asociate direct cu produsul	Cerinţe de suport tehnic şi training
5.	Analiza controalelor la instalarea unui software nou	Elaborarea unui plan de schimbare a software-ului	Proceduri-test pentru verificarea asigurării că schimbările de software nu creează probleme noi
6.	Analiza securităţii software-ului	Proceduri pentru limitarea accesului la sistem	Sunt eliminate toate configurările sistemului de tip default (cele stabilite de furnizorul de software)
7.	Analiza bazelor de date instalate pe platformele software achiziţionate	Proceduri de acces la date partajate	Integritatea bazelor de date

Tabelul 4.7.3. **Analiza bazei de date**

Nr. crt.	Tipul analizei	Conţinut	Evaluare
1.	Proiectarea bazei de date	Verificarea modelului bazei de date	Verificarea entităţilor, cheilor primare şi externe, cardinalităţile relaţiilor
2.	Accesul la baza de date	Analiza accesului principal la baza de date	Dacă baza de date permite alegerea metodelor şi tipurilor de indecşi, atunci ar trebui verificată corectitudinea alegerii
3.	Administrarea bazei de date	Niveluri de securitate pentru toţi utilizatorii, drepturi de acces	Proceduri de backup şi recuperare în caz de dezastre

4.	Interfaţa bazei de date	Verificarea procedurilor de import/export	Asigurarea integrităţii şi confidenţialităţii datelor
5.	Utilizarea cu uşurinţă a bazei de date	Se vor utiliza cereri SQL	Verificarea cererilor SQL

Natura unică a fiecărei reţele face dificilă definirea unor proceduri standard de audit. Totuşi, auditorul poate urmări evaluarea riscurilor reţelei.

Tabelul 4.7.4. **Analiza infrastructurii şi implementarea reţelei**

Nr. crt.	Tipul analizei	Conţinut	Evaluare
1.	Controale fizice	Protecţia componentelor de reţea şi a punctelor de acces	Suporturi hardware de reţea, file serverul şi documentaţia se găsesc în incinte securizate
2.	Teste pentru securitatea fizică	Se verifică securitatea fizică a reţelei	Se obţin copii ale accesului în incinta unde se găseşte serverul pentru persoane autorizate (rezerve)
3.	Controale de mediu pentru componentele reţelei	Echipamentul este protejat de electricitate statică, se asigură aer condiţionat şi controlul umidităţii, UPS	Se verifică dacă file serverul, backup-urile sau alte sisteme de salvare de siguranţă din incintă sunt bine păstrate
4.	Teste pentru controale de mediu	Se testează factorii de mediul în care se găseşte serverul	Temperatură, umiditate, electricitate, incendiu
5.	Controale de securitate logică a reţelei	Utilizatorii au parole unice, acces limitat la resurse, securizarea logică combinată cu securizarea hardware	Parolele sunt schimbate periodic, fiecare utilizator are acces doar la resursele necesare pentru îndeplinirea atribuţiilor prestabilite de conducere, noile tehnologii permit utilizarea cheilor hard în combinaţie cu accesul logic pentru a asigura accesul la reţea
6.	Teste de securitate logică	Se testează pe eşantioane drepturile de acces la resurse	Se verifică activitatea utilizatorului în rapoartele întocmite automat de sistem

Controalele de mai sus sunt valabile pentru orice tip de reţea. La nivelul reţelei LAN, această analiză mai adaugă şi controalele următoare:
- verificarea topologiei LAN şi a arhitecturii reţelei;
- componentele LAN semnificative (rutere, switch-uri, hub-uri şi modem-uri);
- topologia reţelei (configuraţia internă a LAN-ului);
- utilizatorii LAN (incluzând aplicaţiile cele mai importante din reţea şi traficul pe care îl dau reţelei);
- administratorul LAN;
- grupurile importante din reţeaua LAN, politicile de securitate pe fiecare grup.

Tabelul 4.7.5. **Analiza controlului operării în reţea**

Nr. crt.	Tipul analizei	Conţinut	Evaluare
1.	Crearea, implementarea şi testarea unui plan al operării în reţea	Procedurile din acest plan sunt create pentru a se asigura controlul efectiv asupra componentelor hardware şi software	Planul operării este utilizat pentru recuperarea şi repornirea unor procese ale utilizatorilor locali din reţea
2.	Politici şi proceduri de securitate	Datele importante din reţea vor fi criptate	Securitatea (parţială sau totală) este asigurată de un singur utilizator, care este sau nu factor de decizie în societate

Analiza operării SI ar trebui să includă observaţii ale personalului privind îndatoririle acestuia pentru a asigura eficienţa operării, stabilirea standardelor şi politicilor, supervizarea adecvată, integritatea datelor şi securitatea.

Tabelul 4.7.6. **Analiza operării SI**

Nr. crt.	Tipul analizei	Conţinut	Evaluare
1.	Acces al operării	Acces la fişiere, la codul sursă, librării, utilitare pentru stabilitatea sistemului	Limitarea la accesul operării
2.	Planificarea operării pe calculator	Operatorii trebuie să înregistreze şi să planifice activităţi pentru procesare	Planificare manuală sau automată
3.	Proceduri pentru obţinerea aprobării scrise sau electronice	Operatorii trebuie să obţină aprobări scrise sau electronice, să înregistreze cererile şi să le analizeze	Evaluarea cererilor pentru a determina procedurile cele mai potrivite

4.	Reluarea executării operaţiilor	Proceduri ce trebuie să reia executarea anumitor activităţi	Se asigură fişierele de intrare şi subrutinele
5.	Accesul la bibioteci	Acest acces la biblioteci ar trebui să fie restricţionat pentru personalul autorizat	Se asigură evidenţa accesării bibliotecii
6.	Conţinutul şi locaţia stocărilor	Stocări de tip media şi date	Stocarea ar trebui să fie făcută în altă locaţie, decât unde se găseşte sistemul operaţional

Pentru a controla primirea/trimiterea de fişiere trebuie stabilite proceduri specifice, care vor fi evaluate de auditor atât din punct de vedere al conformităţii cu standardele, cât şi al autorizării conducerii.

Controlul intrării datelor include: autorizarea intrării documentelor, segregarea atribuţiilor între persoana care controlează datele şi persoana care analizează acurateţea acestora şi erorile. Procedurile de audit determină: conformitatea controalelor, rapoarte ale controlului, forme de autorizare ce conţin semnături.

Tabelul 4.7.7. **Operaţii de ieşire**

Nr. crt.	Tipul analizei	Conţinut	Evaluare
1.	Acces de la distanţă la consola principală	Software ce permite accesul de la distanţă în mod automat	Acest acces este nepermis pentru marea majoritate a operatorilor unui SI
2.	Planuri de urgenţă ce permit identificarea procedurii de dezastre	Procedurile pentru operaţii automate sau manuale	Documentare şi testare adecvată pentru a putea fi recuperate
3.	Programe de aplicaţii	Schimbarea controalelor şi accesul la controale	Operaţii vitale ale SI sunt executate de sistem. Testarea software-ului trebuie făcută periodic, mai ales după actualizări ale sistemului

Tabelul 4.7.8. **Analiza raportului privind problemele de administrare**

Nr. crt.	Tipul analizei	Conţinut	Evaluare
1.	Proceduri utilizate	Înregistrarea, evaluarea şi rezolvarea problemelor operării sau procesării	Proceduri adecvate pentru analiza serviciilor
2.	Performanţa înregistrărilor, motive de întârziere şi proceduri de culegere a datelor statistice	Probleme ce apar în timpul proceselor on-line, asigurarea că analiza este completă şi corectă	Validarea acestora
3.	Determinarea problemelor procesării	Departamentul IT stabileşte proceduri pentru procesarea datelor	Identificarea, verificarea şi soluţionarea completă a problemelor de administrare
4.	Documentarea operării	Asigurarea că procedurile au fost dezvoltate pentru probleme nerezolvate la cel mai înalt nivel de administrare a SI	Validarea procedurilor

Tabelul 4.7.9. **Analiza raportului privind disponibilitatea şi utilizarea hardware**

Nr. crt.	Tipul analizei	Conţinut	Evaluare
1.	Plan de monitorizare a performanţelor hardware	Probleme apărute în jurnal, planificarea proceselor, planificarea mentenanţei, rapoartele activităţii conturilor sistemului	Raport privind validitatea proceselor
2.	Planificare preventivă a mentenanţei	Frecvenţa mentenanţei prescrise	Urmărirea mentenanţei propusă de furnizorul de hardware
3.	Verificarea parametrilor de funcţionare a echipamentului	Contactarea furnizorului	Echipamentul nu funcţionează la parametrii normali
4.	Rapoarte de utilizare şi disponibilitate a hardware-ului	Planificare adecvată pentru cerinţele utilizatorului	Resursele SI sunt disponibile pentru procesarea aplicaţiilor care cer un nivel mare de disponibilitate a resurselor

Planificarea analizelor presupune:

- obținerea unei liste cu aplicațiile planificate, cum ar fi: termene, timpul de pregătire a datelor, timpul estimat pentru procesarea datelor;
- analiza jurnalului consolei (log-uri) pentru a determina dacă s-a respectat planificarea;
- analiza planificării pentru a determina dacă prioritățile procesării au fost stabilite pentru fiecare aplicație;
- determinarea identificării aplicațiilor critice;
- determinarea procedurilor planificării utilizate pentru utilizarea resurselor calculatoarelor;
- analiza procedurilor pentru colectarea, raportarea și analiza indicatorilor de performanță, așa cum au fost definiți la nivelul fiecărui serviciu.

Noile sisteme și servicii sunt instalate în mod frecvent, fără să asigure condiții pentru utilizarea datelor și a resurselor. De aceea, auditul infrastructurii și operării identifică dacă serviciile existente furnizează valori organizației, asigură că datele pot fi utilizate în condiții de maximă securitate.

4.8. Test de evaluare a cunoștințelor

1. Un instrument de diagnosticare a rețelei, care monitorizează și înregistrează informații despre rețea este:
   a. monitorul on-line;
   b. raportul privind timpul de nefuncționare (downtime report);
   c. raportul help desk;
   d. analizorul de protocoale.

2. Care dintre următoarele afirmații este cea mai probabilă cauză pentru ca un server de mail utilizat să genereze spam-uri:
   a. instalarea unui open relay server;
   b. activarea POP3 (*Post Office Protocol*);
   c. utilizarea SMTP (*Simple Mail Transfer Protocol*);
   d. activarea conturilor de utilizatori.

3. Care dintre următoarele afirmații prezintă cel mai mare risc privind monitorizarea jurnalelor de audit ?
   a. jurnalele nu sunt salvate periodic;
   b. sunt înregistrate evenimente de rutină;
   c. procedurile pentru activarea jurnalelor nu sunt documentate;
   d. sunt înregistrate acțiuni neautorizate ale sistemului, dar nu sunt investigate.

4. Care dintre următoarele caracteristici ale unei rețele este cel mai direct afectată de instrumentele de monitorizare a performanței acesteia:
   a. integritatea;

b. disponibilitatea;
c. completitudinea;
d. confidenţialitatea.

5. Verificarea de bază a software-ului pentru autorizare este o activitate adresată:
   a. managementului proiectului;
   b. managementului configurării;
   c. managementului incidentelor de tip problemă;
   d. managementului riscului.

6. Procedurile de management al schimbării sunt stabilite de conducerea SI pentru:
   a. controlul deplasării aplicaţiilor din mediul de testare în mediul de producţie;
   b. controlul operaţiilor de întrerupere a activităţii din lipsa acordării atenţiei cuvenite problemelor nerezolvate;
   c. asigurarea operaţiilor de neîntrerupere a activităţii în cazul unui dezastru;
   d. verificarea că schimbările sistemului sunt bine documentate.

7. Utilizarea software-ului de audit pentru a compara codul obiect a două programe este o tehnică de audit utilizată pentru a testa programul din punct de vedere:
   a. logic;
   b. schimbări;
   c. eficienţă;
   d. calculaţie.

8. Primul pas în managementul riscului unui atac este:
   a. evaluarea impactului vulnerabilităţii;
   b. evaluarea probabilităţii ameninţărilor;
   c. identificarea resurselor informaţionale critice;
   d. estimarea pagubelor potenţiale.

9. Care dintre următoarele topologii ale unei reţele este subiectul pierderii totale a conectivităţii dacă unul dintre calculatoare este în pană:
   a. stea;
   b. magistrală;
   c. inel;
   d. conectare completă.

10. Care dintre următoarele medii de transmisie oferă cea mai bună securitate împotriva accesului neautorizat ?
   a. sârma de cupru;
   b. cablul torsadat;
   c. cablul optic;
   d. cablul coaxial.

Capitolul 5

Securitatea sistemelor informaționale

Capitolul 5
Securitatea sistemelor informaţionale

5.1. Managementul securităţii SI

Cu toate că ameninţările în spaţiul virtual sunt, într-o mare măsură, aceleaşi ca în lumea reală (de exemplu, frauda, furtul, vandalismul şi terorismul), ele sunt mult mai periculoase, având o eficienţă sporită, deoarece atacurile se execută automat de la distanţă, internetul nu are margini şi utilizează tehnici de propagare rapidă.

În general, securitatea IT presupune implementarea de măsuri specifice pentru protecţia mediului IT (calculatoare, reţele, sisteme informaţionale şi baze de date) împotriva atacurilor intenţionate (spionaj, sabotaj, crimă etc.) sau a oricărui tip de distrugere accidentală. În acest context, în anul 2000, Organizaţia Internaţională de Standardizare (ISO) a adoptat Standardul Britanic BS 7799 ca standard internaţional şi l-a publicat sub numele de ISO 17799 - *Cod practic pentru managementul securităţii informaţiei*. În conformitate cu acest standard, sunt identificate 36 de obiective de control şi 127 de elemente de control, grupate în zece categorii:

a) politica de securitate;
b) planificarea continuării afacerii;
c) controlul accesului la sistem;
d) dezvoltarea şi întreţinerea sistemului;
e) securitatea fizică şi a mediului;
f) conformitatea;
g) securitatea personalului;
h) securitatea organizaţiei;
i) managementul calculatoarelor şi al reţelei;
j) clasificarea şi controlul resurselor informatice.

Pentru operaţionalizarea standardului ISO 17799 a fost elaborat standardul BS 7799-2, care permite implementarea unui sistem de management al securităţii informaţiei prin parcurgerea următoarelor etape:

a) definirea sistemului de management al securităţii informaţiei şi a politicilor aferente;
b) stabilirea responsabilităţilor şi resurselor necesare;
c) specificarea activelor şi managementul riscului;
d) administrarea riscurilor;
e) selectarea controalelor;
f) aplicabilitatea;
g) implementarea.

În mod similar, Institutul pentru Guvernanţă IT, care funcţionează sub patronajul ISACA furnizează cele mai bune practici pentru procesele IT prin publicaţia sa COBIT (*Control Objectives for Information and related Technology*). COBIT structurează procesele IT în patru domenii:

a) planificare şi organizare;
b) achiziţionare şi implementare;
c) funcţionare şi suport;
d) monitorizare şi evaluare.

Cele patru domenii enumerate includ 220 de controale, clasificate în 34 de obiective de nivel înalt.

Obiectivele fundamentale de securitate, care se regăsesc printre cerinţele unui mediu de afacere, sunt:

- *confidenţialitatea* – prevenirea accesului neautorizat la informaţii; garantarea procedurilor şi metodelor ca informaţia, care se află în tranzit sau stocată, să fie accesibilă numai entităţilor autorizate să acceseze respectivele resurse;
- *integritatea* – informaţia este protejată de pierderi sau modificarea neautorizată; garantarea procedurilor şi metodelor ca informaţia, care se află în tranzit sau stocată, să nu poată fi modificată;
- *disponibilitatea* – garantarea că entităţile autorizate au acces la resursele informaţionale atunci când au nevoie de ele; de exemplu, prevenirea atacurilor de tip DoS (*Denial of Service*);
- *conformitatea* cu legile, reglementările şi standardele aplicabile.

Implementarea unui sistem de management al securităţii informaţiei oferă o serie de avantaje:

- câştigarea încrederii partenerilor de afaceri (furnizori, clienţi);
- continuitatea afacerii;
- îmbunătăţirea sistemelor de prevenire şi răspuns în caz de incidente;
- minimizarea riscurilor pentru furtul, coruperea sau pierderea informaţiei;
- accesarea în siguranţă a informaţiei (de către angajaţi şi clienţi);
- justificarea şi optimizarea costurilor necesare implementării controalelor de securitate;
- demonstrarea implicării şi angajamentul managementului pentru securitatea informaţiei;
- demonstrarea conformităţii propriilor practici de securitate cu standarde recunoscute;
- conformitatea cu cerinţele legale, cu regulile şi regulamentele locale;
- asigurarea faptului că riscurile şi controalele sunt permanent revizuite.

În prezent, instrumentele pentru audit şi evaluare sunt orientate preponderent către aspectele de bază ale sistemelor şi reţelelor informatice, fără a se acorda atenţia cuvenită problemelor organizaţiilor (politici şi proceduri) sau aspectelor umane (management, cultură, cunoştinţe), factori ce pot avea o influenţă dramatică asupra securităţii infrastructurilor informatice.

5.1.1. Fundamentele managementului securităţii SI

Managementul securităţii informaţiei se defineşte ca fiind ansamblul proceselor de stabilire şi menţinere a unui cadru de lucru şi a unei structuri de administrare care oferă garanţia că strategiile de securitate a informaţiei sunt aliniate şi susţinute prin obiectivele afacerii, sunt în concordanţă cu legile şi reglementările aplicabile pentru administrarea cât mai adecvată a riscurilor.

Este necesar ca personalul care se ocupă cu administrarea securităţii informaţiei într-un departament sau companie să cunoască cerinţele care sunt descrise prin legislaţia, regulamentele şi directivele aplicabile. Mai mult, pentru stabilirea unui management eficient, organizaţiile pot beneficia de cele mai bune practici identificate. Totuşi, companiile trebuie să-şi adapteze practicile de administrare a securităţii informaţiei la misiunea, obiectivele, operaţiile şi cerinţele proprii.

Activităţile de guvernare a securităţii informaţiei se vor integra cu structura şi activităţile specifice ale companiei. Elementele-cheie care facilitează integrarea sunt: planificarea strategică, proietarea şi dezvoltarea organizaţională, stabilirea rolurilor şi responsabilităţilor, arhitectura întreprinderii şi documentarea obiectivelor de securitate prin politici de implementare şi monitorizare (figura 5.1.1).

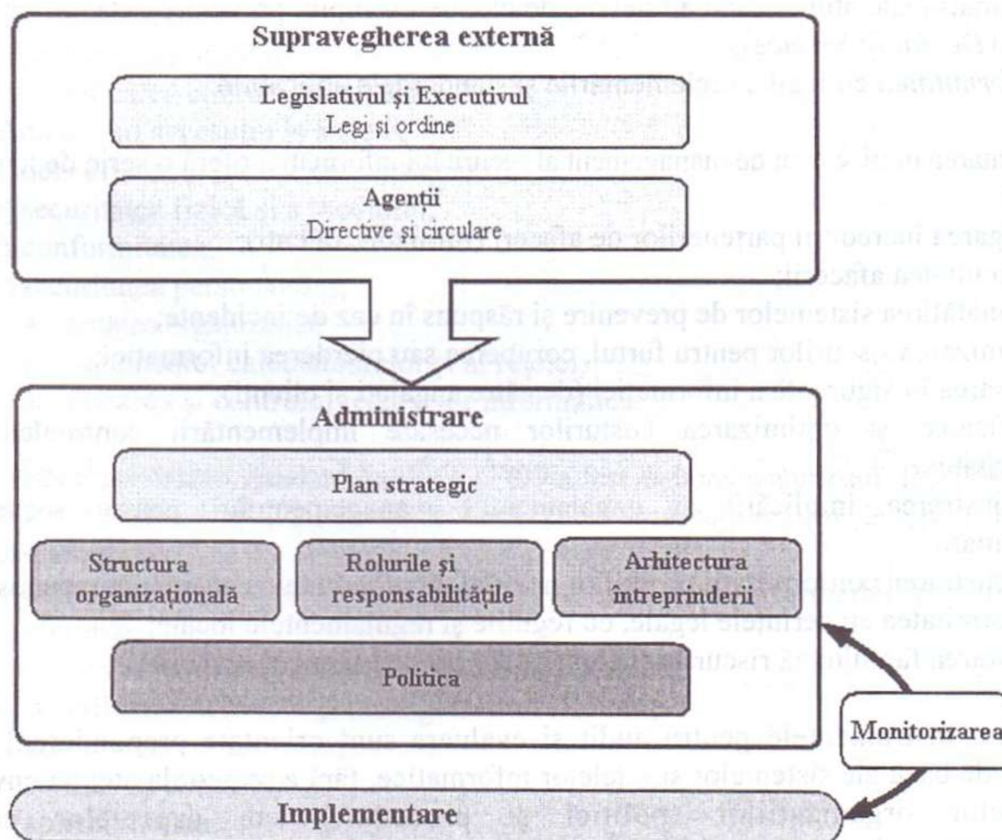


Figura 5.1.1. **Componentele managementului securităţii informaţiei**

Controalele de securitate sunt de trei tipuri:
- *controlul fizic* asigură protecţia mediului IT şi se realizează prin personal de securitate, camere video, lacăte, sisteme de alarmă, surse de alimentare neîntreruptibile;
- *controlul tehnic* se referă la controlul accesului şi include: autorizarea accesului la activele companiei, criptarea;
- *controlul administrativ* se referă la politica de securitate şi procedurile de implementare, ca parte a planului de securitate. De exemplu, un control administrativ poate include: politica, ghidurile de securitate, procedurile de securitate, instruirea în domeniul securităţii.

Implementarea unui sistem de securitate necesită înţelegerea şi analiza riscurilor care pot să intervină asupra mediului IT şi aplicarea celor mai bune măsuri pentru reducerea lor la un nivel acceptabil pentru organizaţie. Pentru identificarea configuraţiei sistemului de securitate propriu este necesar să se proiecteze şi să se implementeze un **plan de securitate**, care va fi parte a planului strategic de dezvoltare a afacerii organizaţiei.

Politica de securitate este componenta centrală a planului de securitate, fiind necesară o documentare şi informare serioase înainte ca propriile controale să fie aplicate mediului IT. O politică de securitate conţine precizarea scopurilor şi a intenţiilor. La o primă vedere, toate politicile de securitate sunt similare, având ca obiectiv prevenirea breşelor de securitate. Elaborarea unei politici de securitate este un proces dificil care presupune adaptarea la specificul organizaţiei. Un pas important pentru implementarea planului de securitate constă în determinarea sistemelor, aplicaţiilor, datelor şi entităţilor care vor fi securizate. După stabilirea politicii de securitate urmează instruirea utilizatorilor, pentru a-i familiariza cu noile reguli de securitate.

O politică de securitate trebuie să specifice în mod clar următoarele aspecte:
- obiectivele organizaţiei privind securitatea: asigurarea protecţiei datelor împotriva scurgerilor de informaţii către entităţi externe, protejarea datelor faţă de calamităţile naturale, asigurarea integrităţii datelor sau asigurarea continuităţii afacerii;
- personalul răspunzător pentru asigurarea securităţii care poate fi: un grup restrâns de lucru, un grup de conducere sau fiecare angajat;
- implicarea organizaţiei în ansamblu la asigurarea securităţii: cine va asigura instruirea în domeniul securităţii, cum va fi integrată partea de securitate în structura organizaţiei.

Pentru atingerea obiectivelor de securitate şi realizarea unui nivel înalt de protecţie, planul de securitate va fi dezvoltat şi implementat pe niveluri. În acest fel modelul conceptual al unui sistem de securitate va include următoarele niveluri (figura 5.1.2):
- *securitatea aplicaţiei* se referă în primul rând la securitatea produselor software care pot fi utilizate pentru dezvoltarea aplicaţiilor de afaceri, ca de exemplu servere web, SSL (*Secure Sockets Layer*) etc.;

- *securitatea sistemului* este implementată la nivelul comenzilor de sistem şi controlează toate funcţiile software ale sistemului. Utilizatorii sunt identificaţi şi autentificaţi la nivel de sistem printr-un singur mecanism de securitate, pentru toate operaţiile pe care le vor executa pe sistem;
- *securitatea reţelei* face parte din proiectarea acesteia şi include controalele prin firewall-uri, VPN (*Virtual Private Network*) şi *gateways*;
- *securitatea fizică* se ocupă de protecţia sistemelor, dispozitivelor şi mediilor pentru backup şi include controalele de acces, sursele de tensiune neîntreruptibile, liniile de comunicaţie redundante;
- *securitatea organizaţiei* este responsabilă pentru toate aspectele planului de securitate a organizaţiei, incluzând politicile de securitate, instruirea în domeniul securităţii, sistemele de afaceri ale organizaţiei şi planificarea pentru recuperare în caz de dezastru.

Planul de securitate oferă un cadru de lucru pentru luarea deciziilor specifice cum ar fi, de exemplu, ce mecanisme de apărare se vor utiliza şi cum trebuie configurate serviciile. Planificarea unui sistem de securitate şi gestionarea vulnerabilităţilor sunt activităţi care implică compromisuri şi optimizări succesive. Planificarea măsurilor de securitate este arta de a găsi un compromis între valoarea relativă a informaţiilor, costul protejării acestora şi probabilitatea ca ele să fie atacate.

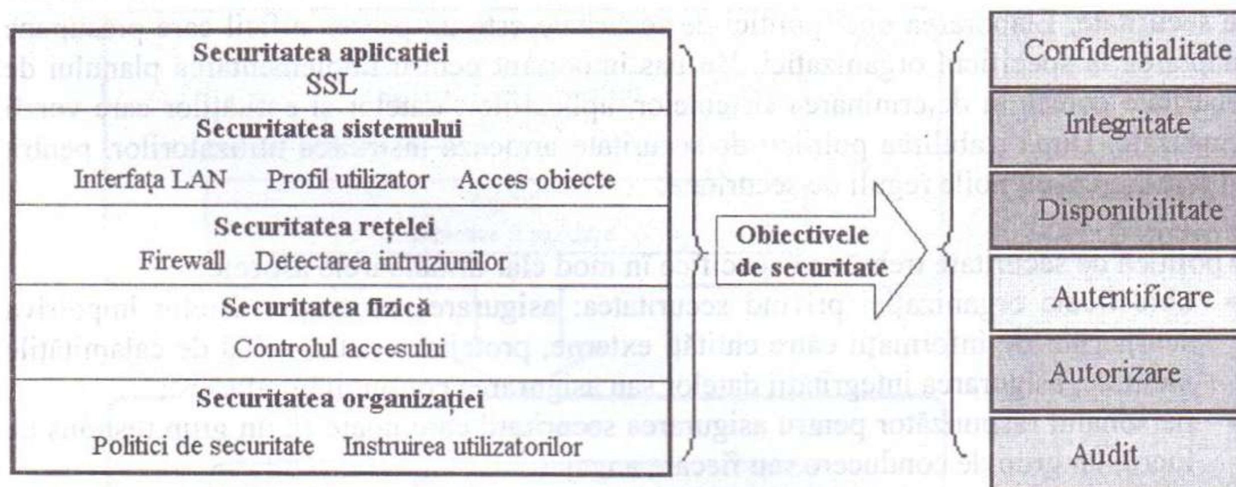


Figura 5.1. 2. **Implementarea securităţii pe niveluri**

5.1.2. Roluri şi responsabilităţi privind securitatea SI

Planul de securitate al unei organizaţiei cuprinde următoarele roluri şi responsabilităţi:

- *comitetul de coordonare a securităţii* stabileşte şi aprobă practicile de securitate. Politicile, ghidurile şi procedurile de securitate afectează întreaga organizaţie, astfel că trebuie să aibă suport şi propuneri din partea utilizatorilor finali, managementului de execuţie, administrării securităţii, personalului SI şi consilierului juridic.
- *managementul de execuţie* are responsabilitatea pentru protecţia generală a activelor informaţionale şi răspunde de implementarea planului de securitate;

- *grupul consultant pentru securitate* are responsabilitatea revizuirii planului de securitate al organizaţiei;
- *ofiţerul şef de securitate* (*Chief Security Officer* – CSO) are un rol-cheie în securitatea sistemului informatic al organizaţiei. El garantează că sistemul informatic este implementat şi se execută în conformitate cu politica de securitate. Ofiţerul de securitate evaluează vulnerabilităţile şi stabileşte măsuri sporite de securitate;
- *ofiţerul şef pentru confidenţialitate* (*Chief Privacy Officer* – CPO) aplică politicile prin care compania asigură drepturile de confidenţialitate pentru informaţiile angajaţilor şi clienţilor;
- *proprietarii de procese/active informaţionale şi date* garantează aplicarea măsurilor de securitate în concordanţă cu politica organizaţiei. De exemplu, proprietarul de date este responsabil pentru protecţia datelor sau activelor informaţionale ale organizaţiei. De obicei, proprietarul datelor face parte din grupul celor care se ocupă cu managementul organizaţiei. Responsabilităţile generale ale proprietarului de date sunt: decide nivelurile de clasificare a datelor, defineşte modul lor de accesare şi cum sunt protejate. Datele pot fi clasificate în: confidenţiale, private/personale, sensitive şi publice;
- *custodele* se ocupă de protecţia activelor informaţionale sau datelor organizaţiei. Această responsabilitate este alocată pentru *controlul accesului logic*. Persoana care îndeplineşte acest rol se mai numeşte *administrator cu securitatea sistemului*;
- *specialistul/consultantul în securitate* îşi aduce contribuţia la proiectarea, implementarea, managementul şi revizuirea politicilor, standardelor şi procedurilor de securitate ale organizaţiei. În mod obişnuit, specialistul în securitate este membru al departamentului IT. Persoana care îndeplineşte acest rol este instruită să lucreze cu proprietarii şi custozii datelor;
- *administratorul cu securitatea sistemului* este responsabil cu implementarea şi întreţinerea controalelor de securitate cerute prin politica de securitate. Activităţile incluse în fişa acestui post de lucru sunt: crearea, reactualizarea şi ştergerea profilelor de utilizatori, alocarea noilor utilizatori la profilele de grup, setarea şi iniţializarea parolelor pentru noii utilizatori, reactualizarea şi revocarea privilegiilor utilizatorilor. De asemenea, administratorul securităţii inspectează fişierele pentru auditul securităţii şi urmăreşte setările de securitate ale sistemului, pentru monitorizarea stărilor de securitate. Dacă se identifică anumite deviaţii de la funcţionarea normală, administratorul de securitate va deschide un raport al incidentului şi va lansa o investigaţie;
- *utilizator*: orice persoană care are dreptul să utilizeze resursele sistemului. Drepturile alocate unui utilizator vor fi în concordanţă cu responsabilitatea pe care o îndeplineşte;
- *partenerii externi* se referă la furnizori şi partenerii de afaceri care se ocupă cu activele informaţionale;
- *dezvoltatorii IT* au responsabilitatea să implementeze securitatea informaţiei în aplicaţiile lor;
- *auditorul* de securitate poate fi un membru intern al organizaţiei sau un membru al unei firme de audit. Un auditor de securitate inspectează în mod regulat procedurile

de securitate ale organizaţiei şi controlează, pentru a fi sigur că sunt îndeplinite, cerinţele din politica, procesele, procedurile şi ghidurile de securitate.

Securitatea informaţiei trebuie să fie integrată încă din etapa de dezvoltare a sistemelor IT, pentru a încerca să protejeze în mod corespunzător informaţia pe care sistemul intenţionează să o transmită, prelucreze şi stocheze. Există o serie de legi şi directive care cer integrarea securităţii în sistemele IT.

5.2. Controlul accesului logic

Controalele accesului logic sunt utilizate pentru a gestiona şi proteja informaţiile. Descoperirea vulnerabilităţii unui control al accesului logic, care poate fi accidentală sau intenţionată, include o parte de natură tehnică şi una de natură organizaţională. Expunerile logice sunt activităţi neautorizate care se întrepătrund cu procesarea normală cum ar fi: modificarea datelor şi a software-ului, blocarea serviciilor utilizatorilor, distrugerea datelor, compromiterea utilităţii sistemului, perturbarea proceselor, urmărirea fluxului de date sau activitatea utilizatorilor, bazelor de date sau aplicaţii.

Acestea includ:

- *scurgerea de informaţii (data leakage)*, care poate fi accidentală prin lăsarea nesupravegheată sau intenţionată a resurselor, care poate fi de exemplu copierea fişierelor din calculator;
- *înregistrări de pe reţea (wire tapping)*, care presupun captarea de informaţii ce sunt transmise la nivelul unei reţele;
- *cal troian (Trojan horses)/ieşire de urgenţă (backdoor)* este un cod ascuns ce se execută ori de câte ori se execută programul autorizat în care s-a infiltrat, deschizând mai multe porţi virtuale pe calculatorul infectat, permiţând astfel intrarea hackerilor în sistem;
- *viruşii (viruses)* sunt coduri de program malițioase inserate în alte coduri executabile ce se pot autoexecuta;
- *viermii (worms)* sunt programe ce pot distruge datele sau utilizează în mod anormal procesele sistemului de operare, dar care nu se autoexecută aşa cum se întâmplă în cazul viruşilor;
- *bombele logice (logic bomb)* nu se autoexecută, acestea necesitând date suplimentare, cum ar fi programarea atacului sau modificarea datelor într-un timp specificat;
- *interzicerea serviciului (denial-of-service)* presupune întreruperea sau interzicerea accesului la servicii a utilizatorilor, reţelelor, sistemelor sau alte resurse;
- *închiderea calculatorului (shutdown)*, proces iniţiat prin conectarea de la alt calculator prin tehnica remote[1];

[1] Tehnica remote se referă la procesarea cu usurinţă a datelor aflate pe un alt sistem decât cel local.

- *war driving* permite interceptarea datelor prin ataşarea unui calculator de tip laptop la reţeaua wireless;
- *piggybacking* este un act de urmărire a unei persoane autorizate ce accesează o poartă securizată sau un atac electronic la o legătură autorizată pentru a intercepta sau altera transmisii de date;
- *capcanele (trap doors)* sunt puncte de ieşire a codurilor autorizate de sistemul de operare, datorate testelor sau întreţinerii sistemului. Un hacker care a reuşit să penetreze sistemul lasă una sau mai multe capcane pentru a-şi facilita accesul ulterior;
- *atacuri nesincronizate (asynchronous attacks)* determină modificări în modul în care sistemele de operare alocă resursele pentru procese diferite;
- *rotunjirea prin lipsă (rounding down)* presupune ca ceea ce rezultă din rotunjirea în minus a unei sume să fie trimis într-un cont specificat.
- *trunchierea (salami technique)* presupune eliminarea unor cifre de la partea zecimală a unei sume şi trimiterea acestei valori într-un cont specificat. Diferenţa dintre rotunjirea prin lipsă şi trunchiere constă în faptul că cea de-a doua sustrage o valoare mai mare decât prima. Spre exemplu, suma 3,238 RON, utilizând *rotunjirea* prin lipsă devine 3,235 (se sustrage valoarea 0,003), iar prin *trunchiere* poate deveni 3,200 (se sustrage 0,035).

Strategia de implementare a programelor antivirus

Cea mai importantă problemă în implementarea unui program antivirus este stabilirea căilor de intrare a viruşilor. Odată ce au fost depistate şi catalogate ca fiind vulnerabilităţi maxime, căile de intrare a viruşilor sunt comparate cu modulele de scanare ale programului antivirus ce urmează a fi implementat. Fiecare utilizator va putea avea acces la un program antivirus. De asemenea, este recomandat să se implementeze un singur program antivirus, deoarece, la un moment dat, codurile de căutare ar putea fi catalogate ca fiind virus de către celălalt program antivirus.

Se recomandă ca la instalarea programului antivirus să se creeze un orar de scanare a sistemului. Antivirusul va trebui să pornească automat şi va raporta administratorului de sistem dacă au fost identificate amprente de viruşi şi dacă au putut fi îndepărtate cu succes din sistem. Actualizarea programelor antivirus este obligatorie, fiind necesară actualizarea bazei de date cu amprente de viruşi noi, ori de câte ori este nevoie.

În alegerea unui program antivirus se va avea în vedere şi tipul de lucru, în reţea sau local, cu „ieşire" la internet sau doar în reţeaua LAN, VPN etc. pentru fiecare tip de lucru în parte trebuind să existe un modul de scanare. Programul antivirus va fi ales în aşa fel încât să nu îngreuneze lucrul în sistemul în care este instalat (RAM, HDD). Mai nou, programul antivirus se găseşte într-un pachet complet cu firewall şi sisteme de criptare, compatibile cu lucrul în reţea sau local.

Căile de acces logic la infrastructura unei organizaţii pot fi la nivelul unui singur PC sau la nivelul unei reţele. La nivelul unui PC, utilizatorii intră direct în sistem şi aplicaţii, fiind monitorizaţi mult mai uşor. În cazul unei reţele LAN, resursele acesteia trebuie să fie partajate pentru utilizatori în funcţie de natura sarcinilor de serviciu. Complexitatea accesului la resurse creşte odată cu numărul de echipamente din reţea şi cu nevoia de parcurgere mai puţin securizată sau nesecurizată a mediului IT, cum este internetul.

Punctele generale de intrare controlează accesul la reţeaua de calculatoare a organizaţiei şi sunt de tip consolă şi staţii de lucru on-line (sau terminale). Aceste puncte de intrare sunt similare cu arhitectura client/server şi se pot concretiza în:

- *conectivitatea reţelei*, unde accesul este dat de legătura la calculator asupra unui segment din infrastructura reţelelor organizaţiei şi presupune identificarea şi autorizarea utilizatorului la un server de domeniu;
- *accesul de la distanţă* (*remote access*) este controlat prin identificarea şi autorizarea utilizatorului la acea parte din infrastructură pe care o accesează. Pentru acces la toate componentele reţelei este necesară implementarea unei reţele virtuale private (VPN).

Controalele de acces software sunt unele dintre cele mai critice controale pentru a asigura protecţia resurselor unei organizaţii. Prin urmare, acestea trebuie să existe la toate nivelurile de acces ale arhitecturii sistemelor, incluzând reţele, platforme sau sisteme de operare, baze de date şi aplicaţii. Fiecare dintre aceste componente ale arhitecturii sistemelor cere identificarea şi autorizarea utilizatorilor, autorizarea accesului la partajarea resurselor şi prezintă rapoarte ale activităţii acestora.

Identificarea şi autentificarea în controlul accesului software sunt procese care permit stabilirea şi identificarea identităţii celui care accesează aplicaţiile software. Pentru aceasta se impune stabilirea celor mai frecvent întâlnite vulnerabilităţi, care pot fi exploatate de intruşi:

- metode de autentificare slabe;
- potenţialul utilizatorilor de a trece de mecanisme de autentificare;
- lipsa confidenţialităţii şi integrităţii pentru informaţiile stocate;
- lipsa criptării pentru autentificarea şi protecţia informaţiilor transmise în reţea;
- lipsa cunoştinţelor utilizatorilor asupra riscurilor asociate cu elemente de autentificare partajate.

ID (identificarea) şi parola sunt componente ale procesului de identificare şi autentificare a utilizatorului. Sistemul de operare poate memora o listă a ID-urilor şi un set de reguli de acces, fiind totodată cel care va da în mod implicit un set de reguli pentru fiecare categorie de utilizator în parte (administrator, guest, utilizator etc.).

Administratorul de sistem este cel care va face politica de parolare pentru utilizatori. Astfel, vor fi creaţi utilizatorii şi fiecare dintre aceştia va primi o parolă generică ce trebuie schimbată la prima intrare în sistem. Parola schimbată trebuie să conţină caractere

alfanumerice, caractere speciale, minuscule, majuscule, într-o combinaţie greu de ghicit. Niciodată nu va conţine nume cunoscute ale membrilor familiei sau alte elemente ce caracterizează utilizatorul (marca maşinii preferate, numele animalului de companie etc.) şi nici nu se va lăsa un bileţel pe monitor cu parola, aşa cum se întâmplă în unele organizaţii. De asemenea, setările vor determina actualizarea periodică a parolei, durata de timp fiind determinată de nivelul de securitate ce trebuie asigurat.

O notă aparte în politica stabilirii parolelor trebuie acordată administratorului de sistem. Parolele din punctele-cheie sunt unice. Acesta va face notări cu privire la parole, pe hârtie (agendă) şi nu electronic, care va fi închisă într-o locaţie sigură. În această locaţie nu are acces decât administratorul şi încă o persoană din conducerea organizaţiei, pentru a se putea asigura securizarea parolelor de acces nu numai la resurse, dar şi la date şi aplicaţii.

Cea mai cunoscută metodă de identificare şi parolare, în momentul de faţă, este accesul la infrastructură pe baza **cardurilor sau cheilor hard (chei USB)**, în combinaţie cu ID şi parolă. O altă posibilitate de recunoaştere a identităţii utilizatorului o poate reprezenta utilizarea caracteristicilor biometrice (voce, amprentă digitală etc.), însă acest tip de identificare prezintă şi anumite limite: nu se mai poate identifica identitatea utilizatorului, dacă, spre exemplu, geometria amprentei digitale a fost modificată în urma unui accident sau în cazul identificării vocii, dacă utilizatorul are fluctuaţii în intensitarea vorbirii cauzate de o simplă răceală.

Gestionarea elementelor biometrice se adresează securităţii colecţiilor, distribuirii şi procesării datelor biometrice ce cuprind:

- integritatea, autenticitatea şi nonrepudierea datelor;
- gestionarea datelor biometrice în timpul existenţei, transmiterii şi stocării datelor, verificării, identificării şi terminării proceselor;
- utilizarea tehnologiei biometrice, incluzând compararea unu la unu sau unu la mai mulţi, pentru identificarea şi autorizarea utilizatorilor;
- aplicarea tehnologiei biometrice la nivel intern sau extern, la fel ca şi controlul accesului fizic şi logic;
- încapsularea datelor biometrice;
- tehnici pentru transmisii sigure şi stocări de date biometrice;
- securitatea fizică hardware utilizată într-un ciclu de viaţă biometric;
- tehnici pentru integritatea şi protecţia datelor biometrice.

Utilizatorii cer, de regulă, relaţii de încredere între aplicaţii şi sistem. Astfel, un utilizator ce a intrat în sesiunea de lucru nu va fi obligat să se identifice şi autorizeze pentru fiecare aplicaţie, mai ales atunci când lucrează cu o serie de aplicaţii. **Single sign-on (SSO – o singură indentificare şi autorizare)** poate fi definit ca totalitatea proceselor de autentificare şi autorizare asupra tuturor platformelor utilizate printr-o singură funcţie. Această funcţie utilizează interfeţele apropiate arhitecturii client/server, sistemelor distribuite, sistemelor vitale, securitatea reţelelor incluzând şi mecanismele de acces la distanţă (*remote access*).

Avantajele pe care le prezintă aceasă funcţie sunt următoarele:
- utilizatorul nu este nevoit să memoreze multe parole;
- îmbunătăţeşte abilităţile administratorului în gestionarea conturilor utilizatorilor şi autorizării acestora în toate sistemele;
- reduce sarcina suplimentară a administratorului de sistem în reactualizarea parolelor uitate;
- reduce timpul utilizatorilor pentru intrarea în multiplele sesiuni de lucru.

Dar această funcţie poate avea şi o serie de dezavantaje cum ar fi: costul asociat implementării funcţiei este ridicat, centralizarea semnăturilor de acces într-un singur punct poate compromite datele din sistem, suporturile pentru fiecare mediu al sistemului de operare este dificil de implementat.

Procesul de autorizare utilizat pentru controlul accesului cere ca sistemul să fie capabil să identifice şi să diferenţieze utilizatorii. Administrarea securităţii accesului logic poate fi făcută într-un mediu centralizat sau descentralizat. Avantajele securităţii într-un mediu descentralizat sunt:
- administrarea securităţii este realizată dintr-o singură locaţie pentru toate locaţiile distribuite;
- problemele de securitate sunt rezolvate într-un timp mai scurt;
- controalele de securitate sunt monitorizate în mod frecvent.

Riscurile asociate responsabilităţii distribuite în administrarea securităţii includ posibilitatea ca standardele locale să fie implementate mai puţin decât cele cerute de organizaţie, nivelurile de gestionare a securităţii să fie sub cele cerute de administrarea generală, ceea ce duce la indisponibilitatea controalelor conducerii şi a auditului.

Accesul de la distanţă (*remote access*) este cerut de organizaţii pentru ca tipuri diferite de utilizatori să aibă acces la resurse, cum ar fi: angajaţi, consultanţi, parteneri de afacere, clienţi etc. Utilizând această metodă de acces, sunt puse la dispoziţia utilizatorilor o serie de metode şi proceduri. Accesul la distanţă presupune utilizarea resurselor atât în cadrul aceleiaşi organizaţii, cât şi la nivelul unui concern. Din acest punct de vedere, se impune stabilirea configurării optime pentru protocolul TCP/IP, care va asigura funcţionarea la parametrii normali ai reţelei. La nivelul unui concern, se impune implementarea reţelei VPN, care să asigure şi securitatea accesului la distanţă.

Metodele de conexiune cel mai des întâlnite privind accesul la distanţă sunt **conexiunea dial-up** şi **reţele dedicate**. Conexiunea dial-up prezintă avantajul unui cost scăzut, dar în acelaşi timp dezavantajul că nu poate fi implementată la nivelul unei organizaţii, fiind foarte lentă ca viteză de lucru. Avantajul reţelelor dedicate la nivelul unei societăţi este acela că are o rată de performanţă ridicată, datorită liniilor de telecomunicaţii dedicate. Un dezavantaj al acestor reţele îl prezintă costul ridicat, de două până la cinci ori mai mare decât în cazul conexiunilor la internet.

Riscurile accesului de la distanţă includ:
- interzicerea serviciului atunci când utilizatorii nu au drept de acces la date sau aplicaţii;
- lipsa configurării comunicaţiilor la nivel software;
- lipsa configurării instrumentelor ce fac parte din infrastructură;
- probleme de securitate fizică a utilizatorilor.

Controalele accesului la distanţă includ politici şi standarde, autorizări, mecanisme de identificare şi autorizare, instrumente şi tehnici de criptare, cum este VPN, gestionarea reţelei şi a sistemului.

În cazul accesului utilizând PDA (*Personal Digital Assistant* – asistent digital personal) trebuie precizat faptul că o serie de organizaţii utilizează aceste instrumente pentru un acces mai rapid la date. De aceea, se impun probleme de control, după cum urmează:
- PDA trebuie să respecte cerinţele de securitate aşa cum au fost definite la nivel de organizaţie;
- configurarea şi utilizarea PDA ar trebui actualizate în permanenţă şi controlate;
- angajaţii ar trebui instruiţi, atunci când utilizează un astfel de instrument;
- pregătirea angajaţilor trebuie să includă şi politici şi ghid de utilizare a instrumentelor PDA;
- aplicaţiile pentru aceste instrumente sunt cele care nu modifică arhitectura reţelelor, pentru care există licenţă şi care sunt instalate şi configurate de tehnicieni bine documentaţi în acest scop;
- PDA care stochează date importante pentru societate trebuie să aibă implementat şi un sistem de criptare a datelor;
- ameninţările asociate PDA sunt la fel ca cele pentru laptop sau computere (exemplu: viruşi etc.);
- utilizarea camerelor web presupune politici implementate pentru cuplarea/decuplarea acestora;
- PDA autorizate pentru afaceri trebuie să fie înregistrate într-o bază de date, pentru a face diferenţa dintre instrumentele PDA proprii afacerii şi cele ale clienţilor.

Atunci când sunt utilizate tehnologii mobile (*flash memory*, *hard mobil* etc.), care nu necesită decât conectarea *plug and play*, pentru a muta date de pe reţele pe sisteme independente sau invers, pot apărea o serie de riscuri ce trebuie eliminate prin politica de securitate, mergându-se până la interzicerea utilizării unor astfel de dispozitive.

Cele mai multe controale de acces la software conţin rapoarte sau jurnale care sunt completate automat, pe niveluri de acces, dată, timp, utilizator, privind procesele care au fost rulate cu succes şi cele care au avut erori, precum şi motivul pentru care s-a produs eroarea. Dreptul de acces la un astfel de jurnal trebuie atent controlat de administratorul de sistem. Restricţionarea şi monitorizarea accesului sunt elemente ce vor apărea în jurnal, ori de câte ori apare o problemă de securitate a sistemului. În acest caz,

vulnerabilităţile sistemului vor putea fi monitorizate, pentru a putea fi eliminate în timp util din sistem.

Din punct de vedere al accesului la copiile de siguranţă a datelor, trebuie menţionat faptul că fiecare mediu de salvare are şi vulnerabilităţile asociate, ce trebuie îndepărtate. Aceste medii de stocare pot fi: hard disc, bandă magnetică, floppy disc, CD sau DVD. În manevrarea acestor medii, se va ţine seama de o serie de precauţii, şi anume: se va evita lumina puternică, aceste medii vor avea etichete şi vor fi protejate la scriere, vor fi ţinute departe de câmpuri electromagnetice sau electrostatice, şocuri sau vibraţii etc.

5.3. Securitatea reţelelor LAN şi a aplicaţiilor client-server

Comunicarea în reţea include, de regulă, instalarea şi utilizarea echipamentelor de reţea (PC-uri, imprimante, rutere, repertoare etc.). Pentru aceasta, se impune stabilirea unor principii privind controalele securităţii, cum sunt:

- funcţiile de control ale unei reţele trebuie să fie executate de operatori/tehnicieni calificaţi;
- funcţiile de control ale unei reţele trebuie separate, iar sarcinile se execută prin rotaţie;
- software-ul care realizează controlul reţelei trebuie să aibă acces restricţionat la funcţii de ştergere sau modificare şi să întocmească un jurnal al tuturor activităţilor;
- auditul funcţiilor de control trebuie să fie verificat în permanenţă pentru a detecta operaţii neautorizate;
- standardele şi protocoalele trebuie să fie documentate şi puse la dispoziţia operatorilor;
- accesul la reţea trebuie monitorizat în permanenţă de către inginerii de sistem pentru a detecta accesul neautorizat;
- trebuie întocmite analize ale reţelei pentru a se verifica, din timp în timp, dacă s-a modificat eficienţa reţelei şi timpul de răspuns al unor procese;
- trebuie utilizat un sistem de criptare a datelor în reţea pentru a proteja mesajele în timpul transmiterii.

Aceste controale sunt valabile pentru reţele LAN ce au o conexiune dial-up, wireless sau conexiune prin cablu.

Primul element şi cel mai important în securizarea reţelelor LAN îl reprezintă filtrarea traficului la nivelul unei reţele ce se poate face cu programe de tip firewall sau cu servere Proxy. Acestea permit sau nu, în funcţie de configuraţie, accesul unui proces în internet.

Un **firewall** este un sistem sau un grup de sisteme care gestionează controlul accesului între două reţele. Mai multe detalii despre firewall vor fi descrise la subcapitolul 5.5. Sunt utilizate două mecanisme: primul constă în interzicerea traficului şi al doilea în autorizarea acestuia. Multe firewall-uri lasă să treacă doar curierul electronic (poşta). În

această manieră, sunt interzise toate celelalte atacuri în schimbul atacului bazat pe serviciul de poștă. Alte firewall-uri mai puțin stricte blochează în mod unic serviciile recunoscute ca fiind servicii periculoase.

În general, firewall-urile sunt configurate pentru a proteja împotriva accesului neautorizat din rețeaua externă. Acesta împiedică hackerii să utilizeze o sesiune de lucru în rețeaua internă, dar autorizează utilizatorii să comunice liber cu exteriorul.

Firewall-ul constituie un punct unic unde auditul și securitatea sunt predefinite în concordanță cu politica de securitate globală a rețelei. De exemplu, un site care va conține informații strict secrete din cadrul unei companii nu va avea ieșire la internet, acesta servind doar pentru angajații companiei. O altă problemă importantă împotriva căreia un firewall nu are cum să lupte este omul. Există persoane din interiorul organizațiilor care, cu scopul de a face rău sau chiar cu intenția de a vinde secretele de serviciu, ocolesc firewall-ul sau chiar schimbă configurările.

Firewall-urile nu depistează viruși. Sunt alte metode, de a verifica fișierele, pentru a putea fi transferate în rețea în siguranță. Un firewall nu va putea înlocui atenția și conștiința utilizatorilor care trebuie să respecte un număr limitat de reguli, banale de altfel, pentru a putea evita problemele apărute. Prima regulă și cea mai importantă este aceea de a nu deschide niciodată un fișier atașat la un e-mail fără a fi sigur de proveniența lui.

Trebuie să luăm măsuri globale și importante împotriva virușilor. Fiecare stație de lucru trebuie să aibă instalat un antivirus (virușii pot fi transmiși prin internet, dar și pe alte suporturi de date, cum ar fi dischete, CD-uri, unități mobile de memorare). Societățile care pun în vânzare software de tip firewall asociază acestuia și un antivirus. Exemplu concludent în acest sens ar fi Norton Antivirus și Norton Firewall.

Din cele prezentate mai sus, desprindem o concluzie esențială, și anume că la configurarea unui firewall va trebui să avem în vedere următoarele reguli:

- politica globală de securitate va fi aleasă de organizație;
- niveluri de control vor stabili cine este autorizat și cine are interdicție;
- din punct de vedere financiar, trebuie ales un firewall care să îndeplinească o bună parte din cerințele politicii de securitate (un cost mic al firewall-ului poate duce la o configurare și administrare anevoioasă).

Serverul Proxy servește la izolarea unuia sau mai multor calculatoare pentru a putea fi protejate (figura 5.3.1).

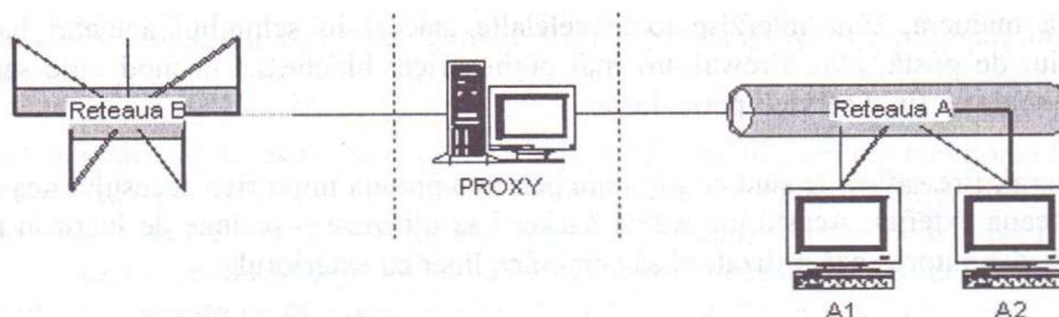


Figura 5.3.1. **Serverul Proxy**

Calculatoarele din rețeaua A trebuie să se conecteze la rețea prin intermediul unui server Proxy. Acesta din urmă, asigură legătura între rețele și calculatoarele de protejat. De asemenea, calculatoarele din rețeaua B nu vor comunica direct cu rețeaua A, ci cu serverul Proxy. Pentru aplicațiile din rețeaua B, adresa IP a clientului va fi cea a serverului Proxy. Spre exemplu, atâta timp cât avem o conexiune la un server HTTP, browser-ul se va conecta la serverul Proxy și va cere să se afișeze URL-ul (identificatorul uniform al resurselor). Serverul Proxy este cel care va gestiona cererea și care va returna rezultatul browserului. De asemenea, serverul Proxy va obliga toate cererile să treacă prin el, reducând numărul de porturi care nu-i corespund. Un server Proxy are avantaje suplimentare în materie de performanță. Dacă doi utilizatori cer în același interval de timp aceeași pagină, aceasta va fi memorată în serverul Proxy și va fi încărcată mult mai rapid la o cerere ulterioară. Serverul Proxy poate filtra cererile în funcție de regulile impuse.

Rețelele LAN pentru marile companii sunt foarte greu de administrat. Rețeaua virtuală locală (VLAN - *Virtual Local Area Network*) vine astfel în ajutorul managerilor IT, permițând adaptarea rețelelor la schimbări fără a reduce performanțele acestora. O rețea virtuală este un grup de calculatoare, servere și alte resurse de rețea, care se comportă ca și cum au fost conectate la un singur segment de rețea, chiar dacă nu se „văd" între ele. Această grupare logică a rețelei, pe noduri, ajută managerii IT să nu mai impună restricții de lucru suplimentare asupra rețelelor și nici un cablaj suplimentar, ceea ce duce ulterior la o arhitectură mai simplă, o administrare și un control mult mai rapid în rețea. VLAN permite o mare flexibilitate, eficiență în segmentul de rețea, permite utilizatorilor și resurselor să fie grupate logic, fără a putea vedea locația fizică.

La fel de important, VLAN ajută la atingerea performanțelor necesare prin segmentarea rețelei în mod eficient. Traficul pe segmente de rețea va fi mai mic, în consecință rețeaua va fi mai puțin aglomerată, deci pachetele transportate mai rapid, iar în acest moment intervine o problemă foarte importantă: **securitatea**. Ea este necesară atunci când pachetele se schimbă între VLAN-uri, acestea trecând prin rutere (măsură standard de securitate, care restricționează accesul la rețele).

Din punct de vedere hardware, un *sistem de protecție* foarte important este sistemul RAID (*Redundant Array of Independente Disks*) matrice redundantă de discuri

independente, prin care datele sunt distribuite pe două sau mai multe unităţi de hard disc şi în paralel sunt duplicate pe mai multe discuri din matrice. Redundanţa garantează faptul că în cazul unui incident nu se vor pierde date. Există două posibilităţi de a pune în aplicare sistemul RAID: o soluţie hardware şi una software. Un *sistem securizat de tip RAID nu protejează datele* împotriva intruşilor sau în cazul virusării sistemului, motiv pentru care trebuie făcută o copiere a datelor pe suporturi externe. Aceste suporturi pot avea legături cu o altă staţie de lucru din reţea sau suport mobil (CD-ROM, DAT, HDD mobil etc.).

Elementele critice ale reţelei trebuie *protejate* de calamităţi naturale. Pentru aceasta se impune respectarea regulilor privind protejarea serverelor, plasarea resurselor hard într-un loc sigur. De asemenea, garanţia sau depanarea hardware trebuie asigurate, astfel încât să nu se blocheze procesul de prelucrare a datelor.

Dacă un serviciu al unui server trebuie să fie accesibil în mod permanent, atunci acesta va fi *protejat*. Singura soluţie de asigurare permanentă a serviciului este de a dubla resursele. Pentru un server putem pune în aplicare un sistem cu *cluster*, care este un grup pe calculatoare independente, cunoscute ca noduri, care colaborează pentru a asigura disponibilitatea aplicaţiilor şi a resurselor necesare clienţilor. Putem folosi două servere, unul să răspundă clienţilor, iar celălalt să fie folosit pentru a asigura o permanenţă a serviciilor. Cele două servere sunt legate între ele în aşa fel încât toate informaţiile de pe primul se găsesc şi pe al doilea. În cazul în care unul dintre servere se defectează, celălalt preia toate serviciile (figura 5.3.2).

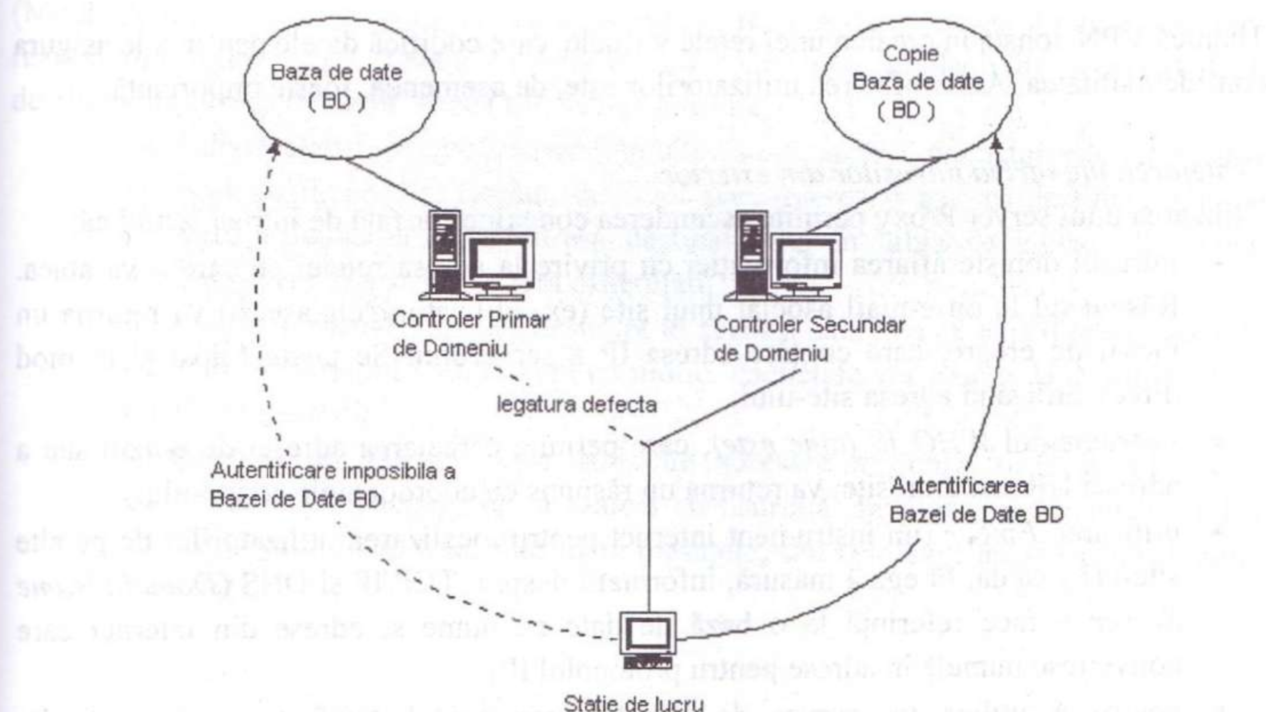


Figura 5.3.2. **Circuitul datelor în cazul folosirii a două servere**

Controlul accesului la sistemul informatic presupune stabilirea următoarelor reguli:
- staţiile de lucru trebuie să fie accesate, în mod unic, de *utilizatorii* acestora (filtrarea utilizatorilor);
- una dintre sursele de risc al vulnerabilităţii unei staţii de lucru este instalarea suplimentară de aplicaţii neautorizate;
- utilizatorii nu-şi vor ţine parolele scrise pe hârtii lăsate pe birou la îndemâna oricui.
- staţiile de lucru trebuie să fie sigilate fizic pentru a evita accesul la hard disc şi/sau componente esenţiale;
- serverul trebuie protejat, în mod particular, prin interzicerea accesului persoanelor în încăperea unde se află acesta;
- accesul liber la BIOS-ul calculatorului poate duce la schimbări de configurare şi deci la nefuncţionarea staţiei de lucru;
- strategiile sistemelor de operare permit limitarea posibilităţii utilizatorilor sau staţiilor de lucru.

Securitatea transferului de date

Accesul la date de la distanţă se face doar dacă utilizatorul are drept de acces la acestea. În cazul unui utilizator mobil, care accesează datele, există mai multe riscuri, în comparaţie cu un utilizator care foloseşte o staţie de lucru fixă (informaţiile tranzitează între organizaţie şi utilizatorul mobil într-un mod public uşor de spionat).

Tehnica VPN constă în crearea unei reţele virtuale, care codifică datele pentru a le asigura confidenţialitatea. Autentificarea utilizatorilor este, de asemenea, foarte importantă.

Protejarea împotriva intruşilor din exterior
Utilizarea unui server Proxy permite ascunderea conexiunilor faţă de intruşi, astfel că:
- intrusul doreşte aflarea informaţiei cu privire la adresa reţelei pe care o va ataca. Răspunsul la un e-mail asociat unui site (ex. utilizator@cig.ase.ro) va returna un mesaj de eroare, care conţine adresa IP a serverului. Se poate folosi şi în mod direct, utilizând adresa site-ului;
- instrumentul *WHO IS (cine este)*, care permite cercetarea adresei de e-mail sau a adresei URL al unui site, va returna un răspuns cu coordonatele server-ului;
- utilizarea *Finger* (un instrument internet pentru localizarea utilizatorilor de pe alte site-uri) va da, în egală măsură, informaţii despre TCP/IP şi DNS (*Domain Name Server* – face referinţă la o bază de date cu nume şi adrese din internet care convertesc numele în adrese pentru protocolul IP);
- pentru a utiliza un server de WEB, instrumentul *DOS traceroute* permite cunoaşterea nodului IP;

- un intrus, care încearcă pentru prima oară să intre în sistem poate fi tentat să se desfăşoare ca un utilizator telnet. Dacă primul port nu este accesibil, va scana toate celelalte porturi (deschise sau nu):
- în cazul în care *telnet* funcţionează, trebuie impusă o condiţie de identificare, deoarece intruşii trec în revistă utilizatorii generici, cum ar fi root sau administrator;
- dacă nici de data aceasta nu se poate intra în sistem, se poate folosi FTP şi utiliza un utilizator cu numele server-ului sau adresa IP de primire. Sistemul se va deschide, se va căuta o parolă de reţea sub formă criptată, care poate fi decodată cu ajutorul programelor crack;
- dacă portul FTP este închis sau nu se accesează, atunci intrusul va utiliza adresa electronică obţinută în urma mesajelor de la server;
- odată ce utilizatorul a folosit parola, cu ajutorul unor aplicaţii, orice intrus poate folosi sistemul, printr-o sesiune telnet nouă (aplicaţia a furnizat parola utilizatorului).

Interconectarea printr-o punte

Aşa cum a fost prezentată în capitolul 4, o punte face trecerea între două reţele de acelaşi tip. Aceasta va analiza adresele de destinaţie a pachetelor. Pentru a ajuta pachetele să fie recunoscute, va reţine o tablă de adresare care va indica postul de lucru şi adresa MAC (Media Access Control) a acestuia, ce se găseşte în reţeaua de sub nivelul punţii, aşa cum rezultă din figura 5.3.3. Odată ce adresa unică hardware a plăcii de reţea MAC a destinatarului trece de nivel, există trei cazuri posibile:

1. când destinatarul nu este cunoscut în tabla sa de adrese, pachetul este retransmis la un alt destinatar din reţeaua sa. După parcurgerea şi găsirea destinatarului, se va trece în mod automat adresa destinatarului în tabla de adrese. Pachetele următoare vor fi distribuite fără dificultăţi;
2. în situaţia în care destinatarul este tot în aceeaşi subreţea ca expeditorul, tabla de adresare a punţii nu va interveni cu nimic. Pachetele vor ajunge la destinaţie fără intervenţia punţii;
3. destinatarul de găseşte peste tabla de adresare a punţii şi în cazul acesta transmiterea de pachete se va realiza cu uşurinţă. În plus, puntea poate prelua adrese la care poate transmite toate mesajele, sau cele care nu vor primi mesaje niciodată.

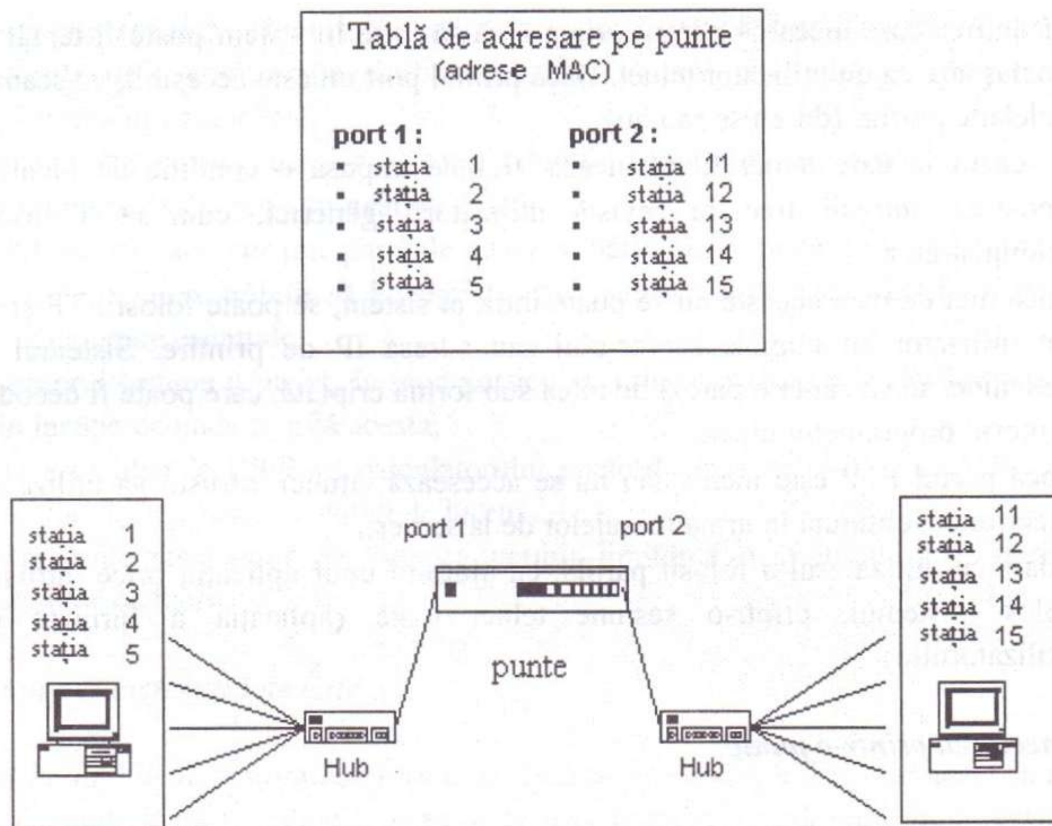


Figura 5.3.3. **Interconexiuni printr-o punte**

Interconectarea printr-un ruter

Ruterul este un dispozitiv care comută pachete la nivelul 3 ISO, în funcţie de adresa IP a destinatarului. El va reţine table de rutare care fac corespondenţa între adresa IP a staţiei de lucru şi porturi, astfel încât pachetele să ajungă pe portul bun. Un exemplu concludent este dat în figura 5.3.4. Ruter-ul serveşte pentru interconectarea reţelelor la distanţă, a subreţelelor de diferite tipuri (*Ethernet, Token ring*) şi asociat switch-urilor ajută la construirea unei reţele VLAN. Ruterele comunică între ele prin utilizarea protocolului RIP (*Routing Information Protocol*), care le permite încărcarea propriilor table de rutare şi deci de a cunoaşte în permanenţă calea cea mai scurtă pentru a ajunge la un alt nod de reţea. În situaţia în care un intrus utilizează informaţii false de routare şi le transmit routerului, acesta va putea redirija informaţii „sigure" şi va răspândi informaţii care nu i-au fost destinate. Aceasta va duce în final la un refuz de acces al serviciului respectiv.

O tehnică de rutare a pachetelor, traversând reţeaua, este aceea de rutare la sursă. În desfăşurarea acestui proces, pachetul care conţine propriile informaţii de rutare şi ruterele nu au propria lor tablă de rutare, până la primirea informaţiilor.
Acest sistem a fost o soluţie de securitate în caz de „spargere" a ruterului. Dacă un intrus construieşte pachete IP de acest tip, va putea să ajungă la staţii de lucru neaccesibile lui până acum şi, bineînţeles, interzise. Este bine să configurăm ruterul în aşa fel încât să nu fie recunoscut acest tip de pachete.

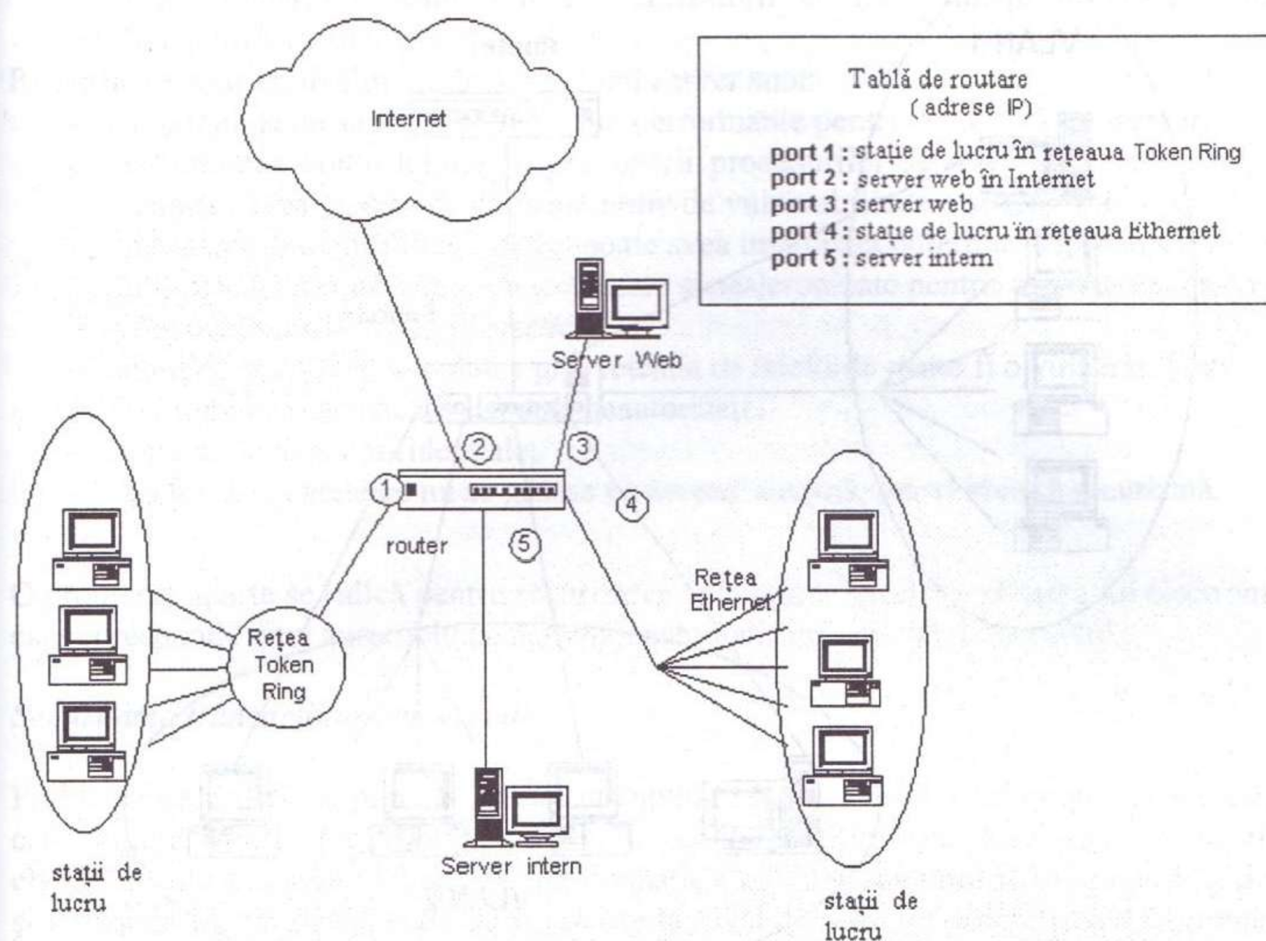


Figura 5.3.4. **Configuraţie cu ruter**

Interconectarea prin switch

Switch-ul este o punte multiport, funcţionează ca o punte cu 12, 24 sau mai multe porturi. Aceste porturi se pot comuta de la nivelul 2 (adrese MAC) la nivelul 3 (adrese IP). Dacă sunt utilizate, switch-urile accelerează traficul şi chiar pot securiza reţeaua sau chiar VLAN.

Un VLAN (figura 5.3.5) este un grup de staţii de lucru ce pot comunica ca şi cum ar fi în aceeaşi reţea fizică, dar pot fi situate oriunde în reţea. Aceasta permite segmentelor logice din reţea să fie sub diferite entităţi şi să obţină o separare totală a acestor entităţi fără să deplasăm partea hard, recablări sau modificări de adrese IP existente. În plus, se optimizează traficul, reţelele virtuale izolează fizic mai multe reţele. Utilizând un ruter sau un switch de nivel 3, VLAN va putea comunica securizat. O execuţie nu va ieşi din VLAN-ul expeditorului dacă destinatarul nu a făcut demersuri pentru primire. Un ruter va fi configurat pentru a face legătura între VLAN-uri.

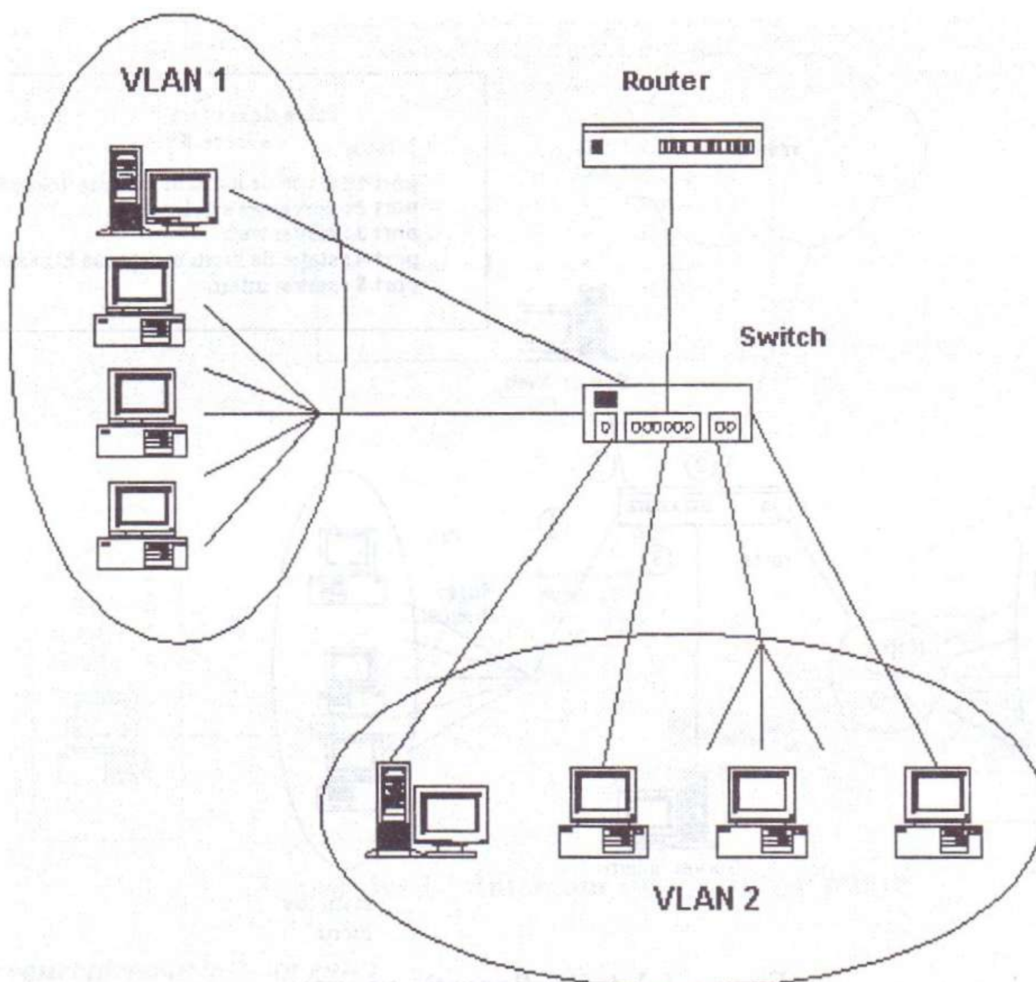


Figura 5.3.5. **VLAN cu switch**

Securitarea aplicaţiilor client-server

O aplicaţie client-server presupune existenţa mai multor puncte de acces. Procedurile de securitate pentru mediul unui astfel de server nu sunt de regulă bine înţelese sau protejate. Sistemele client-server utilizează tehnici distribuite, ceea ce conduce la creşterea riscului de acces neautorizat la datele şi procesele acestuia. Astfel, securizarea unui sistem client-server presupune identificarea tuturor punctelor de acces. Tehnicile de control pentru un sistem client-server sunt:

- securizarea accesului la date sau aplicaţii poate fi asigurată prin dezactivarea unităţilor floppy;
- instrumentele de monitorizare a reţelei sunt utilizate pentru a urmări activitatea de la un utilizator cunoscut la un altul necunoscut;
- utilizarea tehnicilor de criptare a datelor;
- sistemele de autentificare furnizează facilităţi logice care diferenţiază utilizatorii;
- utilizarea unor programe de control al accesului la nivel de aplicaţie şi organizarea utilizatorilor finali reprezintă controale de gestionare care

restricţionează accesul, limitând utilizatorii la acele funcţii necesare pentru îndeplinirea strictă a îndatoririlor.

Riscurile ce apar la nivelul arhitecturii client-server sunt:

- controalele de acces sunt mai puţin performante pentru mediul client-server;
- schimbarea controlului şi a gestionării procedurilor se poate face automat sau manual, ceea ce duce la un prim motiv de vulnerabilitate a sistemului;
- pierderea disponibilităţii reţelei poate avea un impact puternic asupra afacerii;
- utilizarea unor modemuri sincronizate şi nesicronizate pentru conectarea reţelei la alte reţele poate fi neautorizată;
- conexiunea la reţele publice prin reţeaua de telefonie poate fi o vulnerabilitate;
- schimbările de sisteme sau date neautorizate;
- accesul la date confidenţiale;
- codurile şi datele ce nu se găsesc pe aceeaşi maşină, într-o incintă securizată.

O problemă aparte se ridică pentru securizarea aplicaţiilor specifice comerţului electronic, care corespunde unui ansamblu de activităţi automatizate, utilizând internetul.

Securitatea tranzacţiilor comerciale

Problema securităţii se pune la nivelul clientului, reţelei, site-ului informatic al societăţii care comercializează produsele sau serviciile pe internet. Riscurile care apar la nivelul clientului (sau de ordin particular) sunt în relaţie cu divulgarea informaţiilor confidenţiale şi utilizarea ilicită. Problemele de securitate la nivel de reţea se concretizează în termeni de performanţă (timp de răspuns, traficul datelor). Un risc major pentru societate este acela de penetrare a mediului informatic plecând de la site-ul de pe internet, autorizând toate felurile de utilizare a site-ului.

Securitatea conexiunii între cumpărător şi vânzător

Asigurarea securităţii tranzacţiilor comerciale revine nu numai securităţii conexiunii internet între client şi vânzător, dar şi în mod egal serviciului client, altul decât mediul informatic al vânzătorului. O conexiune internet între un navigator şi un server web poate fi stabilită utilizând modulul logic SSL (*Secure Sockets Layer*). SSL este integrat în navigator şi asigură confidenţialitatea.

Principalii operatori ai cărţilor de credit promovează SET (*Secure Electronic Transaction*). Tranzacţia şi numărul cărţii de credit a clientului sunt cifrate de aplicaţie şi sunt transmise vânzătorului. Acesta din urmă va rambursa numărul său de identificare şi cifra de returnare a mesajului înainte de a fi transmis băncii. La recepţie, banca va decoda, autentifica, identifica utilizatorul şi va notifica acordul său vânzătorului care va realiza sau nu tranzacţia cerută. În nici un moment al tranzacţiei, nu va fi public numărul de card şi nu va fi identificat vânzătorul.

Securizarea serverului

Securizarea serverului presupune controlarea cererilor care i-au fost adresate şi securizarea sistemului informatic cu care colaborează pentru a înapoia serviciul solicitat de clienţi. Plecând de la stricta configurare a sistemului, protejarea acestuia de exterior se face de obicei printr-un *firewall*. Configurarea unui *firewall* se face după criteriile de securitate determinate pentru filtrarea traficului parcurs şi astfel se aplică o politică de control al accesului la sistem. Protejarea datelor constă, deci, în limitarea accesului la acestea, precum şi punerea lor la dispoziţia clienţilor autorizaţi.

Trebuie spus că firmele pot apela şi la companii specializate în realizarea de modele de securizare a datelor sau chiar experţi specializaţi în acest domeniu. Cu toate acestea, administratorii reţelei nu vor putea să pună în aplicare şi să menţină funcţional planul elaborat. Organizaţiile trebuie să asigure condiţii materiale şi financiare pentru pregătirea propriilor administratori de reţea şi, astfel, se vor evita situaţiile neprevăzute.

Nu va fi niciodată o posibilă securizarea totală a unui sistem informatic. Hackerii vor descoperi mereu noi vulnerabilităţi de securitate şi vor utiliza aceste noi „fisuri" în sistem. În cazul în care intrusul nu are niciun interes particular pentru o anume societate, se va orienta spre un alt sistem mai uşor de pătruns. Sistemul informatic al organizaţiei evoluează în timp şi se extinde prin noi componente hardware şi software. Odată cu această evoluţie a sistemului, vor apărea şi noi vulnerabilităţi pentru care vor trebui dezvoltate noi soluţii de securizare.

Investind într-un model de securitate complet, vom putea avea sisteme IT mai sigure. Soluţiile de securitate, ca şi politica de securitate de altfel, trebuie gândite global şi nu doar punctual. Nu trebuie uitat faptul că nivelul de securitate a întregului sistem este dat de veriga cea mai slabă. Politica de securitate va trebui actualizată periodic.

5.4. Securitatea în internet

Internetul, această reţea de reţele, este constituit dintr-un ansamblu de infrastructuri, servicii, utilizatori şi resurse informaţionale. Internetul, prin natura sa, fiind un sistem global bazat pe stiva de protocoale TCP/IP prin care se asigură comunicarea între reţelele eterogene publice şi private, este vulnerabil atacurilor. Protocoalele din internet au fost proiectate pentru adresarea şi rutarea pachetelor de date prin reţea. Nu au fost prevăzute mecanisme pentru garantarea sau evidenţa eliberării mesajelor; nu se face verificarea adresei; cel care emite un mesaj nu va şti dacă mesajul a ajuns la destinaţie în timpul în care este cerut; cel care recepţionează nu va şti dacă mesajul a sosit chiar de la adresa specificată în pachet ca adresă de returnare. Ulterior au fost create alte protocoale pentru a elimina unele dintre aceste dezavantaje.

5.4.1. Ameninţări asupra securităţii reţelei

Securitatea unei reţele de calculatoare poate fi ameninţată prin acţiuni cu sau fără rea-intenţie. Astfel, calamităţile naturale, defectarea unor echipamente, erorile de operare sunt incluse în categoria acţiunilor fără o intenţie distructivă. Altele, în schimb, intră în categoria acţiunilor rău-intenţionate. Sursa ameninţărilor poate fi în interiorul sau exteriorul unei reţele private; de asemenea, ameninţările pot fi active sau pasive.

Acţiunile de ***atac pasiv*** au ca scop numai observarea, eventual copierea datelor; intrusul nu va modifica sau şterge datele accesate. Atacurile care pot fi incluse în această categorie sunt:

- **analiza reţelei** (scanarea reţelei) - intrusul aplică în mod sistematic cunoştinţele de amprentare pentru crearea unui profil complet al infrastructurii de securitate a reţelei organizaţiei. Pe durata fazei de recunoaştere iniţială, intrusul utilizează o combinaţie de instrumente şi tehnici pentru întocmirea cataloagelor de informaţie despre reţeaua internă a organizaţiei vizate. Cataloagele pot include informaţii despre numele asociate sistemelor, funcţiile, adresele interne, porţile şi firewall-urile posibile. După ce un sistem răspunde, intrusul va scana porturile sistemului pentru identificarea serviciilor şi sistemului de operare instalate. Ulterior, atacul poate continua prin exploatarea vulnerabilităţilor cunoscute ale sistemului de operare sau ale serviciilor identificate;
- **spionarea reţelei**: intrusul culege informaţia din reţea cu intenţia de a o analiza şi valorifica personal sau să o pună la dispoziţia unei terţe părţi. Aceasta este o particularitate semnificativă când informaţia sensibilă, traversând o reţea, poate fi văzută prin toate celelalte calculatoare, cum ar fi mesaje de e-mail, parole şi, în unele cazuri, ceea ce se tastează în timp real. Aceste activităţi permit intruşilor să obţină acces neautorizat, să utilizeze informaţia, conturile de pe cărţile de credit, să fraudeze şi să compromită confidenţialitatea informaţiilor sensibile ale unei persoane sau organizaţii;
- **analiza traficului** (*ascultarea canalului*): intrusul determină natura traficului între host-urile definite şi prin analiza duratei sesiunilor, frecvenţei, dimensiunea mesajelor poate stabili tipul comunicaţiei care are loc. Metoda se utilizează când mesajele sunt criptate, iar spionarea nu are rezultate.

În cazul ***atacurilor active***, intrusul nu se mulţumeşte numai să acceseze informaţia din reţea, ci va lansa un atac pentru a obţine un control complet asupra sistemului-ţintă sau un control prin care anumite acţiuni de atac se pot realiza. Aceasta înseamnă că, după ce a obţinut accesul neautorizat, atacatorul încearcă să modifice date sau programe, să determine un refuz de serviciu, să obţină privilegii, să acceseze alte sisteme şi să obţină informaţii secrete pentru propriul câştig. Acest tip de penetrare sau intruziune este cunoscut ca un atac activ şi afectează atributele de integritate, disponibilitate şi autenticitate ale securităţii unei reţele. Formele obişnuite ale atacurilor active pot fi:

- **atacul în forţă** (*brute-force*) este lansat prin utilizarea unor instrumente pentru depistarea/spargerea parolelor, care apoi permit accesul neautorizat în reţeaua unei organizaţii;

- **mascarada** (*masquerading*) – intrusul se prezintă cu o identitate falsă pentru a avea acces la date secrete sau resurse ale reţelei, pentru care accesul nu-i este permis cu propria identitate. El poate folosi simultan atât identitatea altei persoane, cât şi adresa IP a unui calculator din reţea (*IP spoofing*) pentru lansarea unui atac de spagere a unui firewall;
- **reluarea pachetelor** (*packet replay*) combină atacul pasiv cu cel activ; în mod pasiv sunt capturate pachetele de date care trec printr-o reţea vulnerabilă sau neprotejată. Aceste pachete sunt apoi inserate într-o reţea ca şi când ar fi un alt mesaj original. Această formă de atac este efectivă când receptorul final al canalului de comunicaţie este automat şi va acţiona pentru recepţia şi interpretarea pachetelor de informaţie fără intervenţia umană;
- **pescuitul** (*fishing*) este un atac prin e-mail în care expeditorul (atacatorul) încearcă să convingă destinatarul că are intenţii serioase şi poate să-l ajute să câştige spre exemplu bani la o loterie, dar pentru aceasta are nevoie de informaţiile personale ale acestuia, contul bancar, PIN-ul cardului etc. Aceste informaţii pot fi folosite ulterior pentru un atac activ;
- **modificarea mesajelor** (*message modification*) se referă la capturarea unui mesaj în vederea modificării neautorizate sau ştergerii (a întregului mesaj sau numai a unei părţi a acestuia), schimbarea secvenţei acestuia sau întârzierea transmisiei către destinaţie. Aceasta poate avea un efect dezastruos dacă, de exemplu, mesajul reprezintă o instrucţiune a unei bănci pentru o operaţie de plată;
- **accesul neautorizat prin internet sau prin servicii care au la bază web.** Multe dintre pachetele software din internet conţin vulnerabilităţi care dau sistemelor subiect pentru atac. În plus, multe dintre aceste sisteme sunt complexe şi dificil de configurat, rezultând un procent mare al incidentelor pentru accesul neautorizat. Exemplele includ :
  - e-mail falsificat;
  - parole `telnet` transmise în clar (de la client la server);
  - alterarea asocierii între adresa IP şi numele de domeniu pentru a întruchipa/a personifica orice tip de server;
  - execuţia script-urilor pe partea de client (prin Java în applet-urile Java), care prezintă pericolul execuţiei unui cod de la o locaţie arbitrară pe o maşină-client;
- **refuzul unui serviciu** (*denial of service*) apare atunci când un calculator conectat la internet este asaltat de foarte multe cereri pentru un serviciu pe care acesta îl oferă şi nu mai poate răspunde (refuză să mai ofere serviciul). În felul acesta sistemul informatic este paralizat, afectând serios clienţii fideli ai acelui serviciu;
- **atacul de penetrare prin apelul telefonic** (*dial-in penetration attack*) – intrusul află numerele de telefon unde se pot obţine informaţii importante despre o companie şi apoi sună un salariat al companiei pentru a-i cere acele informaţii;
- **bombe şi spam-uri prin e-mail** (*e-mail bombing and spamming*) – bombele e-mail constau în transmiterea repetată a aceluiaşi mesaj la un anumit destinatar. Spam-ul e-mail este o variantă de bombă în care acelaşi mesaj este transmis la sute sau mii de destinatari. Acestea pot depăşi capacitatea de memorare a căsuţei poştale a destinatarului;

- **e-mail fals** (*e-mail spoofing*) – un utilizator recepţionează un mail care apare ca având o anumită origine (expeditor), dar în realitate aceasta este falsă (în realitate în spatele mesajului se află un alt expeditor). Spre exemplu, un e-mail care pretinde că vine din partea administratorului de reţea prin care se cere destinatarului să-şi schimbe parola cu una specificată în mesaj, dacă nu face acest lucru este ameninţat cu suspendarea contului.

5.4.2. Controalele de securitate în reţeaua internet

Pentru a stabili controalele de securitate în internet, trebuie să cunoaştem mai întâi care sunt efectele (impactul) şi cauzele produse de exploatarea vulnerabilităţilor reţelei prin atacuri.

Principalele consecinţe ale atacurilor în reţeaua internet sunt:
- pierderea veniturilor;
- creşterea costurilor de recuperare în caz de incidente;
- pierderea unor informaţii de bază ale companiei;
- divulgarea unor secrete comerciale;
- afectarea reputaţiei companiei;
- scăderea performanţelor reţelei;
- încălcarea legilor şi regulamentelor;
- pericolul de a încălca înţelegerile contractuale cu partenerii;
- acţiunile de trimitere în judecată din partea clienţilor pentru pierderea unor date confidenţiale.

Principalele cauze care influenţează atacurile în reţeaua internet sunt:
- disponibilitatea unor instrumente şi tehnici software, comercializabile sau nu, care permit, relativ uşor, reuşita atacurilor la resursele internet;
- lipsa unei conştientizări şi pregătiri a angajaţilor din punctul de vedere al politicilor de securitate din organizaţie;
- exploatarea vulnerabilităţilor cunoscute privind securitatea reţelei şi a sistemelor de operare ale staţiilor de lucru;
- măsurile inadecvate de securitate în privinţa utilizării fără discriminare a serviciilor oferite de internet.

Proiectarea şi implementarea unei reţele la nivelul unei organizaţii trebuie să prevadă controale adecvate pentru prevenirea şi detectarea atacurilor. Auditorul SI trebuie să înţeleagă foarte bine factorii de risc pentru a verifica dacă controalele existente sunt adecvate pentru securitatea SI. Pentru a stabili controalele de securitate privind utilizarea internet, fiecare organizaţie trebuie să stabilească mai întâi regulile de acces la internet în funcţie de cerinţele interne, definind resursele informaţionale ce vor fi disponibile pentru utilizatorii din afara organizaţiei şi drepturile de acces intern şi extern. De asemenea, trebuie clasificate resursele informaţionale din punctul de vedere al senzitivităţii acestora.

Pe baza acestor informaţii, organizaţia poate dezvolta ghidurile şi procedurile de implementare a controalelor necesare pentru a asigura confidenţialitatea, integritatea şi disponibilitatea resurselor informaţionale pe internet.

În plus, deasupra controalelor de securitate, trebuie definite proceduri specifice:

- evaluarea periodică a riscurilor privind dezvoltarea şi reproiectarea aplicaţiilor web;
- conştientizarea şi pregătirea salariaţilor privind securitatea internet, în mod diferenţiat, în funcţie de nivelul de responsabilitate pe care îl au în companie;
- implementarea unei arhitecturi de firewall-uri în concordanţă cu standardele în domeniu;
- implementarea unui sistem de detectare a intruşilor (IDS) conform standardelor;
- accesul de la distanţă pentru coordonarea şi controlul accesului prin dial-up la resursele organizaţiei;
- tratarea incidentelor şi recuperarea erorilor;
- managementul configurării pentru controlul securităţii în cazul unor schimbări în sistem;
- tehnicile de criptare folosite pentru protecţia informaţiilor transmise pe internet;
- controlul asupra informaţiilor afişate pe ecranele staţiilor de lucru;
- monitorizarea activităţilor internet pentru utilizarea neautorizată şi informarea despre incidentele apărute.

5.5. Sisteme de securitate prin firewall

Un firewall este un ansamblu constituit din hardware şi software, care, utilizate împreună, previn accesul neautorizat într-o reţea sau o parte a unei reţele. Componenta *hardware* a unui firewall, în mod obişnuit, este un calculator sau un dispozitiv dedicat pe care se execută funcţiile de control. Componenta *software* este reprezentată prin diverse aplicaţii, care realizează controale de securitate în punctele vulnerabile dintre reţeaua internă a organizaţiei şi internet.

Un firewall deţine cel puţin două interfeţe, una orientată pentru controlul traficului spre exterior (internet) şi cealaltă direcţionată pentru controlul traficului către reţeaua internă (figura 5.5.1).

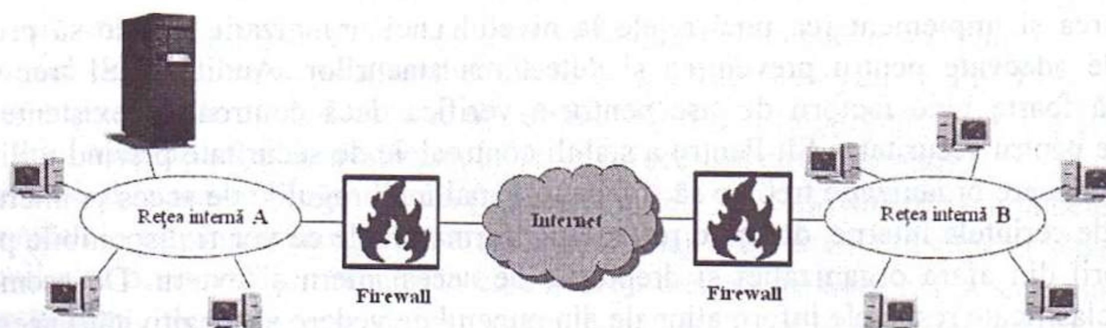


Figura 5.5.1. **Controlul traficului prin firewall**

Firewall-urile pot fi clasificate după:
- nivelul modelului de referinţă OSI la care operează;
- modul de implementare.

Nivelul funcţional, al modelului de referinţă OSI la care operează firewall-ul constituie cel mai utilizat criteriu pentru clasificare. Astfel, tipurile de firewall-uri disponibile pot fi grupate în următoarele trei categorii:
- filtrarea pachetelor - filtrarea pachetelor prin ruter (nivel reţea);
- verificare cu stare completă - *stateful inspection* (nivel transport);
- sisteme firewall la nivel de aplicaţie (nivel aplicaţie).

După modul de implementare, firewall-urile se pot împărţi în două mari categorii:
- *dedicate*: dispozitivul pe care rulează software-ul pentru control este dedicat acestei operaţiuni şi este practic inserat în reţea (de obicei chiar după ruter); are avantajul unei securităţi sporite;
- *combinate:* cu alte facilităţi de reţea; de exemplu, un ruter îndeplineşte şi funcţii specifice unui firewall. În cazul reţelelor mici, acelaşi calculator poate avea, în acelaţi timp, rolul de firewall, ruter, file/print server etc.

Principalele funcţii ale unui firewall sunt:
- blochează accesul la site-uri particulare din internet;
- limitează traficul la unele servicii publice ale organizaţiei (se au în vedere adrese IP şi porturi);
- interzice anumitor utilizatori accesul la unele servere şi servicii;
- monitorizează comunicţiile între reţeaua internă şi o reţea externă;
- monitorizează şi înregistrează toate comunicaţiile între o reţea internă şi lumea exterioară, pentru detectarea încercărilor de pătrundere frauduloasă;
- criptează pachete care sunt transmise între diferite locaţii fizice prin reţele VPN.

5.5.1. Tipuri de firewall

Firewall-ul pentru filtrarea pachetelor este un dispozitiv de rutare care include funcţii pentru controlul accesului pe baza unui set de reguli. Mecanismul de filtrare are capacitatea de identificare a pachetului şi de specificare a modului în care acesta va fi tratat. Un pachet poate fi *acceptat*, *ignorat* (are loc blocarea pachetului fără transmisia unui mesaj de notificare către sursă) sau *refuzat* (blocarea pachetului şi transmisia unui mesaj de notificare către sursă).

Regulile după care acţionează filtrele de pachete sunt stocate în tabele configurate de administratorul de sistem sau ofiţerul de securitate. În aceste tabele sunt specificate adresele IP şi porturile pentru sursele şi destinaţiile acceptate, refuzate şi regulile implicite. Tabelul 5.5.1 prezintă un set de reguli pentru o reţea imaginară a cărei adresă IP este 193.232.3.0 (fiind o adresă IP de clasă C, ultimul număr, 0, reprezintă host-ul din cadrul reţelei şi poate varia între 0 şi 254).

Tabelul 5.5.1. **Set de reguli pentru un firewall cu filtrarea de pachete**

Adresa-sursă	**Port - sursă**	**Adresa - destinaţie**	**Port destinaţie**	**Acţiunea**	**Descrierea**
Oricare	Oricare	193.232.3.0	> 1023	acceptat	Regula permite acceptarea în reţeaua internă a pachetelor-răspuns pentru conexiunile TCP
193.232.3.1	Oricare	Oricare	Oricare	refuzat	Blochează toate conexiunile directe
Oricare	Oricare	193.232.3.1	Oricare	refuzat	Blochează accesul utilizatorilor externi
193.232.3.0	Oricare	Oricare	Oricare	acceptat	Utilizatorii interni pot accesa servere externe
Oricare	Oricare	193.232.3.2	25 (SMTP)	acceptat	Sunt acceptate mesajele de poştă electronică de la utilizatori externi
Oricare	Oricare	193.232.3.3	80 (HTTP)	acceptat	Utilizatorii externi pot accesa serverul web
Oricare	Oricare	Oricare	Oricare	refuzat	Ceea ce nu este acceptat în mod explicit va fi refuzat

Firewall-ul pentru filtrarea pachetelor are două avantaje principale: viteza şi simplitatea. Performanţele firewall-ului sunt în general stabile, regulile de filtrare fiind realizate la nivel de reţea. Firewall-ul operează foarte rapid, deoarece datele corespunzătoare nivelurilor superioare (cele situate deasupra nivelului 3- nivel reţea) ale modelului OSI nu sunt examinate. Prin simplitatea sa, firewall-ul poate fi folosit aproape în orice infrastructură de reţea a unei organizaţii. În afară de viteză şi simplitate, firewall-ul pentru filtrarea de pachete deţine capacitatea de blocare a atacurilor prin refuzul serviciului, fiind ideal pentru plasarea lui la graniţa cu o reţea nesigură.

Firewall-urile pentru filtrarea pachetelor au o serie de puncte slabe:

- nu pot preveni atacurile care exploatează vulnerabilităţile sau funcţiile specifice aplicaţiei, deoarece firewall-ul nu examinează datele nivelului superior. De exemplu, un firewall pentru filtrarea de pachete nu poate bloca o comandă specifică unei aplicaţii;

- funcţia de notificare este redusă, deoarece informaţiile disponibile în firewall sunt limitate. În mod normal, un firewall pentru filtrarea pachetelor conţine informaţii utilizate în luarea deciziilor pentru controlul accesului (adresa sursei, adresa destinaţiei, tip trafic);
- nu suportă scheme avansate pentru autentificarea utilizatorilor;
- în general, sunt vulnerabile la atacuri prin care se utilizează elemente specifice stivei de protocoale TCP/IP, cum ar fi falsificarea adresei nivelului reţea, rutarea prin sursă, fragmentarea unui pachet IP:
  - *falsificarea adresei*: se poate utiliza adresa unui host din reţeua internă sau a unui host dintr-o reţea de încredere. Multe firewall-uri nu pot detecta pachetele în care informaţia de adresare a nivelului 3 a fost alterată. Atacurile de tip *spoofing* sunt folosite pentru a depăşi controalele de securitate implementate într-un firewall. Pentru a elimina falsificarea printr-o adresă IP internă, firewall-ul poate fi configurat să blocheze pachetul pe baza analizei direcţiei fluxului. Dacă atacatorul are acces la o adresă IP externă securizată sau de încredere şi falsifică această adresă, atunci firewall-ul, este depăşit;
  - *specificarea rutei prin sursă*: rutarea prin sursă este mecanismul care permite unui sistem să specifice ruta pe care un pachet IP va trebui să o folosească pentru a ajunge de la host-ul-sursă la host-ul-destinaţie. Din punctul de vedere al securităţii, rutarea prin sursă are posibilitatea să permită unui atacator să construiască un pachet care să depăşeasă controlul prin firewall. Măsura de protecţie recomandată împotriva unei astfel de ameninţări constă în examinarea fiecărui pachet şi dacă este specificată rutarea prin sursă acesta va fi blocat;
  - *fragmentarea unui pachet*: utilizând această metodă, un atacator împarte pachetul IP în unele mai mici, care pot depăşi cu uşurinţă firewall-ul pentru filtrarea pachetelor, deoarece, în mod normal, numai primul din secvenţa pachetelor fragmentate va fi examinat, celelalte vor trece fără să fie inspectate. Se poate elimina acest tip de atac prin configurarea firewall-ului astfel încât să blocheze toate pachetele pentru care fragmentarea IP este disponibilă;
- sunt susceptibile să creeze breşe de securitate printr-o configuraţie necorespunzătoare /improprie, din cauza numărului redus de variabile utilizate în deciziile pentru controlul accesului.

Firewall-urile pentru filtrarea pachetelor sunt foarte potrivite pentru mediile de transmisie la viteză înaltă, unde logarea şi autentificarea utilizatorilor care doresc accesul la resursele de reţea nu este importantă.

Firewall cu monitorizare completă a stării

Firewall cu monitorizare completă a stării (*stateful inspection firewall*) este un filtru de pachete care încorporează elemente suplimentare, specifice nivelului 4 al modelului de referinţă OSI (nivel transport).

Firewall-ul cu monitorizare completă a stării s-a dezvoltat din necesitatea adaptării anumitor aspecte ale stivei de protocoale TCP/IP care fac dificilă utilizarea firewall-urilor

pentru filtrarea pachetelor. Când o aplicaţie creează o sesiune cu un host de la distanţă prin protocolul TCP (serviciu transport orientat pe conexiune), sistemul-sursă îi alocă un port. Scopul este informarea sistemului-destinaţie asupra numărului de port care va accepta răspunsul. Conform specificaţiei TCP, portul-sursă al aplicaţiei-client va fi un număr mai mare decât 1.023 şi mai mic decât 16.384, iar portul pentru aplicaţia server va fi un număr mai mic decât 1.024. De exemplu, pentru serverul SMTP, portul are valoarea 25.

Ruterele pentru filtrarea pachetelor trebuie să permită accesul traficului pe toate porturile mai mari decât 1.023 (pentru serviciile orientate pe conexiune ale nivelului transport) prin care se returnează pachete de la host-urile destinaţie. Deschizând aceste porturi, se creează un imens risc de intruziune a utilizatorilor neautorizaţi, care pot folosi diverse tehnici pentru a abuza de sistem.

Firewall-ul cu monitorizare completă a stării rezolvă această problemă prin crearea unui catalog pentru toate conexiunile TCP solicitate din reţeaua internă, reţinând informaţiile pentru fiecare sesiune căreia îi corespunde unui număr de port mai mare decât 1.023 (tabelul 5.5.2). „Tabela de stare" constituită va fi utilizată pentru validarea traficului către reţeaua internă. Soluţia de verificare a stării complete este mai sigură, deoarece firewall-ul urmăreşte porturile individuale ale aplicaţiilor client, nu permite accesul din exterior pentru toate porturile numere mari. Dezavantajul este că, firewall-ul *stateful inspection* este mai dificil de administrat în comparaţie cu alte tipuri de firewall-uri, datorită complexităţii sale.

Tabelul 5.5.2. **Tabela de stare pentru conexiunile unui firewall *stateful inspection***

Adresă-sursă	Port-sursă	Adresă-destinaţie	Port-destinaţie	Starea conexiunii
193.232.3.100	1030	210.9.88.29	80	Stabilită
193.232.3.102	1031	216.32.42.123	80	Stabilită
193.232.3.101	1033	173.66.32.122	25	Stabilită
193.232.3.106	1035	177.231.32.12	79	Stabilită
...				

Firewall la nivel aplicaţie

Firewall-ul la nivel aplicaţie este un firewall avansat care combină controlul accesului (nivel 3 şi nivel 4) cu funcţionalităţi ale nivelului superior (nivelul 7 – nivel aplicaţie).

Există două tipuri de sisteme firewall la nivel de aplicaţie: *poartă la nivel de aplicaţie* (*application level gateway*) şi *poartă la nivel de circuit* (*circuit level gateway*).

Fiecare *poartă la nivel de aplicaţie*, referită ca un agent *proxy*, comunică în mod direct cu setul de reguli pentru controlul accesului prin firewall, pentru identificarea pachetelor

care au permisiunea să-l tranziteze. Acesta analizează pachetele printr-un set de proxy – unul pentru fiecare serviciu (de exemplu, proxy HTTP pentru traficul web, proxy FTP etc.). Prin modul în care lucrează, performanţele reţelei vor fi reduse. În plus, fiecare agent proxy are abilitatea să solicite autentificarea utilizatorilor de reţea. Autentificarea utilizatorului se poate face în diverse moduri, cum ar fi prin nume utilizator şi parolă, token hardware sau software, adresa sursei sau biometric.

O poartă la nivel de aplicaţie realizează un control la nivel înalt pentru traficul dintre două reţele, în sensul că un serviciu particular poate fi monitorizat şi filtrat în concordanţă cu politica de securitate din reţea. Pentru o anumită aplicaţie, se va instala un cod proxy corespunzător, care va urmări şi administra traficul specific serviciului. Un proxy acţionează ca un server pentru client şi ca un client pentru serverul destinaţie. O conexiune virtuală este stabilită între client şi serverul-destinaţie. Proxy-ul este *transparent* din punctul de vedere al clientului şi al serverului, dar are capacitatea să monitorizeze şi să filtreze orice tip specific de date, cum ar fi comenzile, înainte de a fi trimise către destinaţie. De exemplu, un server FTP permite accesul din exterior. Totuşi, pentru a proteja serverul FTP de anumite atacuri, proxy-ul FTP din firewall va fi configurat să refuze comenzile `put` şi `mput`.

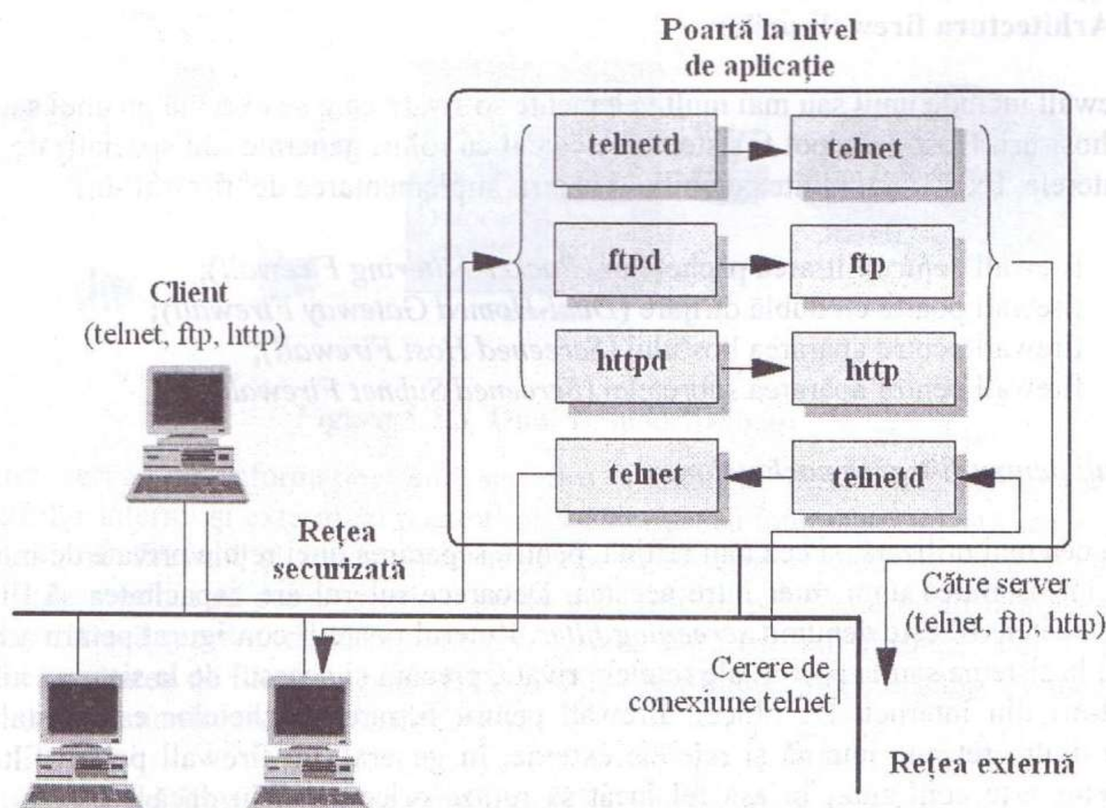


Figura 5.5.1. **Firewall de tip poartă la nivel aplicaţie**

Dacă într-o reţea internă este instalat un proxy, când se lansează o cerere către un server din internet:

- cererea de la un calculator va fi transmisă la serverul proxy;
- serverul proxy contactează serverul de pe internet cu adresa sa, ca adresă-sursă (nu cu a host-ului care a lansat cererea);
- serverul proxy recepţionează datele de la serverul de pe internet şi le transmite host-ului care le-a solicitat.

Adresa IP a unui calculator intern nu va fi cunoscută în afara reţelei. Serverele proxy înregistrează informaţii despre cererile şi transferurile efectuate ca, ulterior, să se poată face o analiză a accesului la internet.

Firewall-urile de tipul *poartă la nivel de circuit* operează tot la nivelul aplicaţie al modelului de referinţă OSI, dar sunt mai eficiente; sesiunile TCP sau UDP sunt validate printr-un singur proxy cu scop general, înainte de deschiderea unei conexiuni. Poarta la nivel de circuit are capacitatea să realizeze o conexiune controlată între un host intern şi altul extern. Mai întâi, se stabileşte un *circuit virtual* între clientul intern şi serverul proxy. Cererile către host-urile din internet sunt dirijate prin circuitul virtual către serverul proxy, iar acesta transmite cererile după ce schimbă adresa IP. Răspunsurile sunt recepţionate prin serverul proxy şi transmise prin circuitul virtual către client.

5.5.2. Arhitectura firewall-urilor

Un firewall include unul sau mai multe elemente software care se execută pe unul sau mai multe host-uri. Host-urile pot fi sisteme de calcul cu roluri generale sau specializate, cum sunt ruterele. Există mai multe posibilităţi pentru implementarea de firewall-uri:

- firewall pentru filtrarea pachetelor (*Packet-Filtering Firewall*);
- firewall poartă cu dublă dirijare (*Dual-Homed Gateway Firewall*);
- firewall pentru apărarea hostului (*Screened Host Firewall*);
- firewall pentru apărarea subreţelei (*Screened Subnet Firewall*).

Firewall pentru filtrarea pachetelor

Soluţia cea mai utilizată, şi cea mai ieftină, pentru separarea unei reţele private de internet constă în instalarea unui ruter între acestea. Deoarece ruterul are capacitatea să filtreze toate pachetele IP este denumit *screening filter*. Ruterul poate fi configurat pentru a bloca accesul la sisteme sau la porturi ale reţelei private, precum şi accesul de la sisteme interne la host-uri din internet. De obicei, firewall pentru filtrarea pachetelor este instalat la graniţa dintre reţeaua internă şi reţelele externe. În general, un firewall pentru filtrarea pachetelor este configurat în aşa fel încât să refuze orice serviciu dacă acesta nu este permis în mod explicit. Cu toate că previne unele atacuri potenţiale, firewall-ul este deschis atacurilor prin vulnerabilităţile rezultate din configurarea şi filtrarea improprie.



Figura 5.5.2. **Ruter pentru filtrarea de pachete (*Screening router*)**

Un *screening filter* este folosit frecvent împreună cu alte instrumente pentru realizarea unui bloc de securitate.

Firewall poartă cu dublă dirijare

Un host pe care este instalat un firewall cu dublă dirijare are cel puţin două interfeţe de reţea şi două adrese IP. Un firewall dual-homed, în configuraţie normală, acţionează pentru blocarea sau filtrarea unei părţi sau a întregului trafic care încearcă să treacă de la o reţea la alta. Pachetele vor traversa firewall-ul printr-un serviciu proxy sau SOCKS[2].

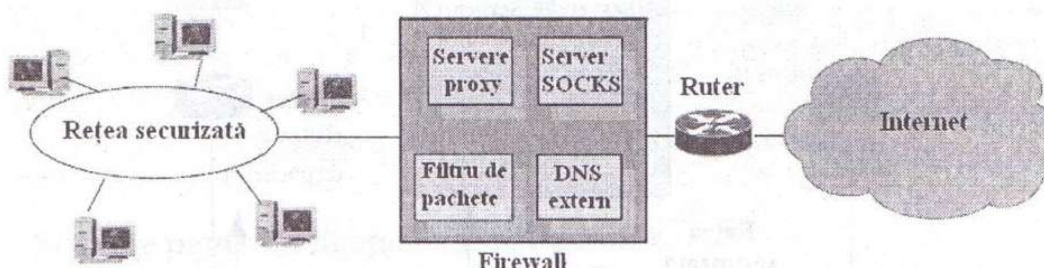


Figura 5.5.3. **Dual-homed firewall**

Dacă un server de informaţie (web sau ftp) trebuie să fie instalat pentru accesul utilizatorilor interni şi externi, el poate fi plasat în reţeaua internă securizată sau poate fi localizat între firewall şi ruter, zonă nesigură. Dacă este instalat în reţeaua internă, firewall-ul va trebui să deţină serviciu proxy prin care se permite accesul la serverul de informaţie. Dacă serverul de informaţie este instalat între firewall şi ruter, ruterul trebuie să aibă capacitatea de filtrare a pachetelor şi să fie configurat corespunzător. Acest tip de firewall este denumit *screened host firewall*.

Spre deosebire de firewall-urile pentru filtrarea pachetelor, firewall-ul cu dublă dirijare va bloca orice atac sosit de la un serviciu necunoscut. Poarta cu dublă dirijare implementează metoda prin care ceea ce nu este specificat ca fiind permis va fi refuzat.

[2] Protocol internet ce permite aplicaţiilor client-server să utilizeze servicii în mod transparent prin firewall-ul reţelei.

Un firewall *dual-homed* este o formă mai restrictivă decât un sistem firewall *screened-host,* în care un host bastion dual-homed este configurat cu o interfaţă pentru serverele de informaţie şi alta pentru host-urile din reţeaua privată.

Screened host firewall

Acest tip de firewall constă dintr-un ruter pentru filtrarea pachetelor şi o poartă la nivel de aplicaţie. Host-ul care include o poartă la nivel de aplicaţie este cunoscut ca un host *bastion*. Ruterul este configurat să transmită întreg traficul nesigur (*untrusted*) către host-ul bastion şi în unele cazuri către serverul de informaţie. Dacă reţeaua internă este în aceeaşi subreţea cu host-ul bastion, prin politica de securitate se permite utilizatorilor interni să acceseze reţele externe în mod direct sau prin utilizarea de servicii proxy. Aceasta se realizează prin configurarea regulilor de filtrare astfel încât ruterul acceptă să transmită spre exterior numai traficul sosit de la host-ul bastion.

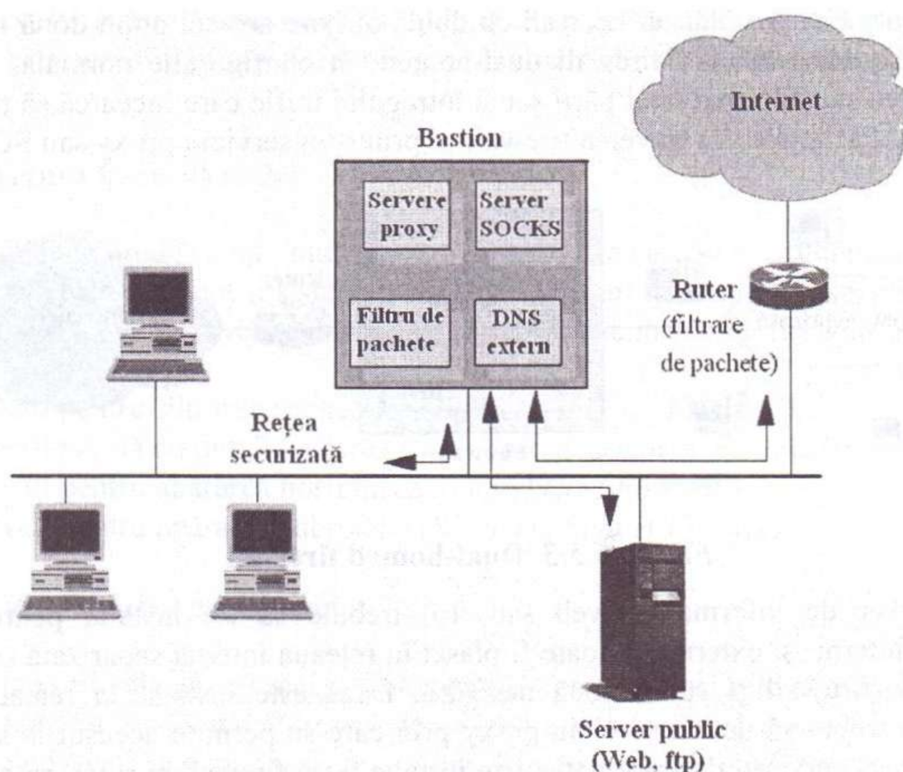


Figura 5.5.4 **Screened host firewall**

Configuraţia constituită dintr-un ruter pentru filtrarea pachetelor şi host-ul bastion permit serverului de informaţie să fie plasat între ele. Prin politica de securitate se stabileşte dacă serverul de informaţie (web, ftp) va fi accesat în mod direct de utilizatorii interni sau externi sau va fi accesat prin host-ul bastion. Dacă este nevoie de o protecţie puternică, traficul către serverul de informaţie, atât din reţeaua internă, cât şi din exterior, va fi dirijat prin host-ul bastion. Host-ul bastion va fi unul standard sau, pentru mai multă protecţie, el poate fi un host dual-homed.

Firewall pentru zona demilitarizată

Firewall-ul constă din două rutere de filtrare şi un host bastion. El realizează un înalt nivel de securitate în comparație cu alte tipuri de firewall, se realizează o zonă demilitarizată (*demilitarized zone* - DMZ) între rețeaua internă şi cea externă.

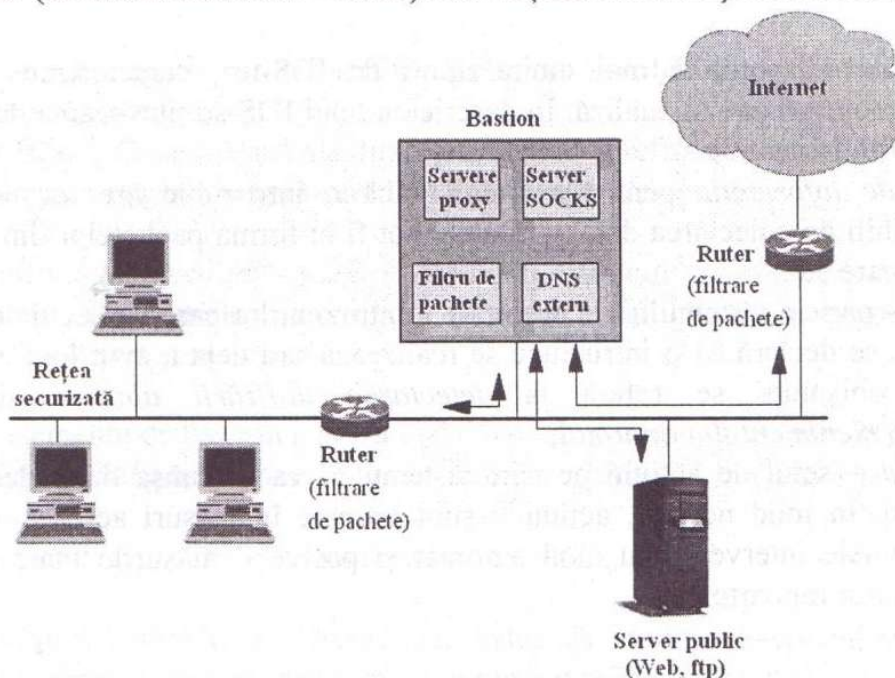


Figura 5.5.5 **Screened subnet firewall**

5.6. Sisteme pentru detectarea intruziunilor

Detectarea intruziunii este procesul de monitorizare a evenimentelor realizate într-un sistem de calcul sau rețea şi analizate pentru semnalizarea încercărilor de compromitere a confidențialității, integrității, disponibilității sau depăşirea mecanismelor de securitate ale unui calculator sau rețea, definite ca fiind *intruziuni*. Intruziunile sunt determinate prin atacurile de acces neautorizat la sisteme din internet sau prin utilizatori autorizați pentru un sistem, care încearcă să obțină mai multe privilegii decât le sunt acordate.

Sistemele pentru detectarea intruziunilor (*Intrusion Detection Systems - IDS*) sunt sisteme software şi hardware care în mod automat procesează şi monitorizează evenimentele apărute într-un sistem sau rețea şi le analizează pentru a semnala problemele de securitate.

Acestea sunt proiectate pentru notificarea şi, în unele situații, pentru prevenirea accesului neautorizat la resursele unui sistem instalat pe un calculator, de cele mai multe ori conectat în rețea. Multe dintre IDS-uri au capacitatea să interacționeze cu firewall-urile în scopul realizării de elemente reactive prin care se oferă serviciu pentru securitatea rețelelor. Firewall-urile care interacționează cu IDS sunt capabile să răspundă, percepând

în mod automat ameninţările de la distanţă, fără să mai intervină întârzierea asociată unui răspuns uman. De exemplu, un sistem pentru detectarea intruziunilor detectează un atac de tipul refuz al serviciului, el poate instrui anumite firewall-uri să blocheze în mod automat mesajele care au ca sursă adresa atacului.

Tipuri de IDS

În prezent sunt disponibile mai multe tipuri de IDS-uri, caracterizate prin diferite elemente de monitorizare şi analiză. În descrierea unui IDS se ţine seama de următoarele componente fundamentale:

- *sursele de informaţie* pentru a stabili dacă o intruziune are loc; senzorii sunt responsabili de colectarea datelor. Datele pot fi în forma pachetelor din reţea, fişiere de notificare etc.;
- *analiza* – parte a sistemului de detectare a intruziunilor care va decide evenimentele prin care se declară că o intruziune se realizează sau deja a avut loc; elementele de analiză obişnuite se referă la *detectarea utilizării abuzive* şi *detectarea excepţiei/evenimentului anormal*;
- *răspunsul* – setul de acţiuni pe care sistemul îl va declanşa după detectarea unei intruziuni. În mod normal, acţiunile sunt grupate în măsuri active – prin care se rezolvă unele intervenţii în mod automat şi pasive – măsurile luate ca urmare a analizei unor rapoarte.

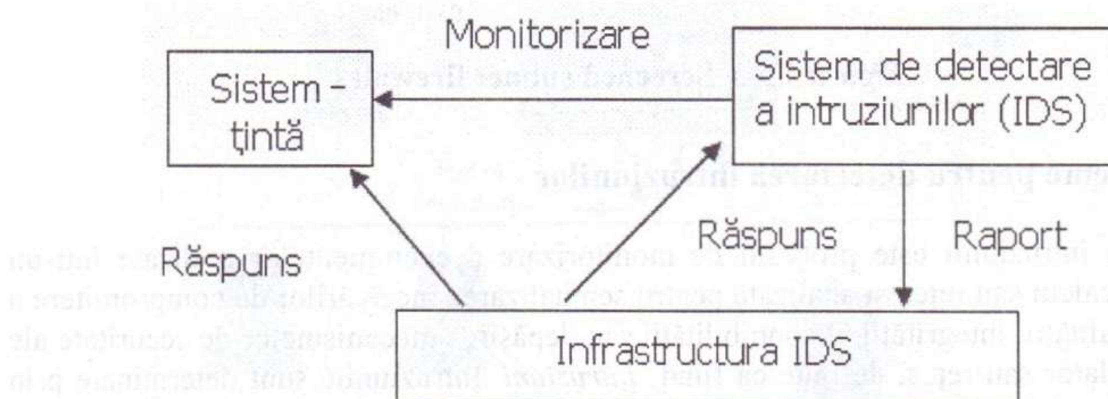


Figura 5.6.1. **Sistemele de detectare a intruziunilor**

Cel mai cunoscut criteriu pentru clasificarea IDS-urilor îl reprezintă ***sursa informaţiilor***. Unele IDS-uri analizează pachetele din reţea capturate pentru identificarea atacurilor, altele analizează informaţiile generate prin sistemul de operare sau software de aplicaţie pentru semnalizarea intruziunilor.

În acest caz, tipurile de sisteme pentru detectarea intruziunilor disponibile sunt:

- IDS-uri bazate pe host (*host-based IDS*) – acestea pot fi instalate pe fiecare sistem de calcul în parte pentru a-l proteja;

- IDS-uri bazate pe rețea (*network-based IDS*) sunt implementate ca analizoare inteligente de protocol; dispozitivele monitorizează traficul care *trece prin* canale, cercetând *semnăturile atacurilor* prin care se determină tipurile de atac în derulare.

Sistemele pentru *detectarea intruziunilor la nivel de host* sunt integrate de regulă în sistemul de operare pentru a-l apăra împotriva atacurilor și posedă următoarele dezavantaje:

- au un impact negativ asupra performanțelor sistemului, datorită numărului mare de parametri analizați;
- nu notifică totdeauna atacurile din rețea, cum ar fi refuzul serviciului;
- au un impact negativ asupra stabilității sistemului de operare.

Sistemul pentru *detectarea intruziunilor din rețea* este mult mai eficient decât un sistem pentru detectarea intruziunilor pentru host, deoarece un singur sistem poate monitoriza o multitudine de sisteme și resurse.

Există două elemente de bază în analiza evenimentelor pentru detectarea atacurilor:

- *detectarea utilizării abuzive* este tehnica utilizată în majoritatea sistemelor comerciale;
- *detectarea excepției* este încă subiect de cercetare.

Detectarea utilizării abuzive analizează activitatea sistemului, observând evenimente sau seturi de evenimente care corespund unui pattern predefinit cu rol de descriere a unui atac cunoscut. Deoarece pattern-urile asociate atacurilor cunoscute sunt denumite *semnături*, detectarea utilizării abuzive este denumită ***detectarea pe bază de semnătură***.

Detectarea excepțiilor identifică comportamentul anormal pe un host sau rețea. Se presupune că, în funcționare, atacurile sunt diferite de activitățile normale (legitime) și pot fi detectate prin sistemele care au capacitatea să identifice aceste diferențe. Detectoarele pentru funcționarea anormală concep profiluri reprezentând comportamentul normal al utilizatorilor, host-urilor sau conexiunilor de rețea. Ulterior, datele colectate sunt analizate și comparate pentru a se determina dacă activitățile monitorizate deviază de la normal.

Măsurile și tehnicile utilizate în detectarea situațiilor anormale includ:

- detectarea pragului, prin care anumite atribute ale comportamentului utilizatorului și sistemului pot fi măsurate (de exemplu, numărul de fișiere accesate de un utilizator într-o perioadă de timp, numărul de încercări fără succes de conectare la un sistem); acesta poate fi static sau euristic;
- măsurări statistice;
- măsurări bazate pe reguli: sunt similare cu măsurările statistice fără parametri;
- alte măsurări, incluzând rețele neuronale și algoritmi genetici.

Honey Pot

Multe produse pentru detectarea intruziunilor sunt în dezvoltare şi vor deveni disponibile. Este important să se înţeleagă cum aceste produse diferă de IDS-urile tradiţionale. *Honey pots* sunt sisteme-capcană proiectate pentru:
- a distrage un atacator de la accesarea unui sistem critic;
- colectarea de informaţii despre activitatea atacatorului;
- încurajarea atacatorului să întârzie pe sistem suficient timp, ca administratorii să raspundă prin contramăsuri.

Avantaje:
- atacatorii pot fi abătuţi de la sistemele-ţintă, pentru a nu le afecta;
- administratorii au timp suplimentar pentru luarea unor decizii de răspuns împotriva atacatorilor;
- acţiunile atacatorilor pot fi uşor şi intensiv monitorizate, iar rezultatele pot fi utilizate pentru rafinarea modelelor şi îmbunătăţirea sistemelor de protecţie;
- *honey pots* pot folosite la identificarea celor care spionează reţeaua.

Dezavantaje:
- implicaţiile legale pentru utilizarea acestor dispozitive nu sunt bine definite;
- *honey pots* nu sunt suficient prezentate pentru a fi utilizate în tehnologia de securitate;
- un atacator expert, odată direcţionat către un sistem-momeală, poate deveni mai agresiv prin acţiunile sale distructive asupra sistemelor organizaţiei;
- un înalt nivel de expertiză este necesar pentru administratorii şi managerii de securitate în a comanda utilizarea acestor sisteme.

Conceptul de *honeynet* desemnează un ansamblu de *honeypots* interconectate, pentru a simula o infrastructură de reţea.

5.7. Studiu de caz privind securitatea unei reţele LAN

Descrierea reţelei care trebuie securizată

O reţea locală formată dintr-un server şi două staţii de lucru (Y, Z) sunt conectate la un hub şi mai departe prin intermediul unui ruter se conectează la internet (figura 5.7.1). Pe server se găsesc informaţii importante, care ar putea fi de folos firmelor concurente, precum şi o bază de date utilizată de angajaţi în diverse aplicaţii.

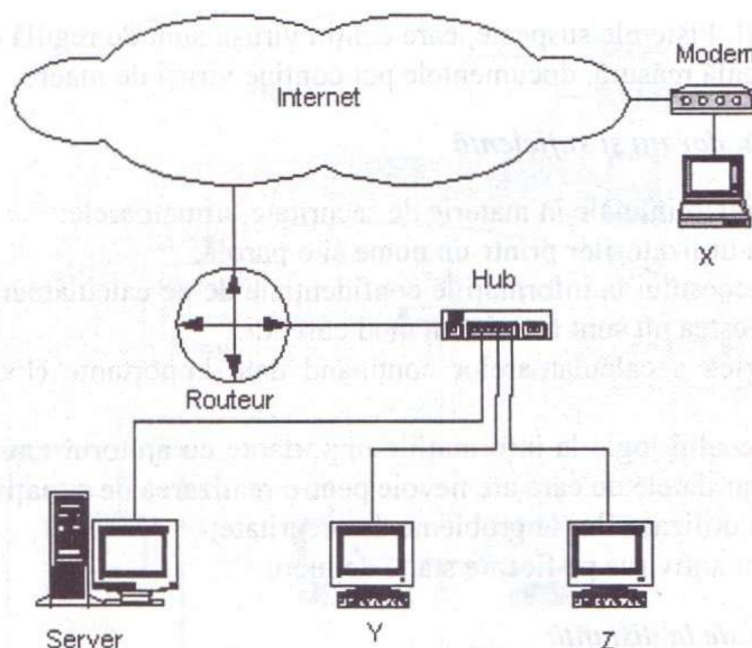


Figura 5.7.1. **Reţea de calculatoare nesecurizată**

Identificarea informaţiilor care trebuie protejate

O bază de date este utilizată de mai mulţi angajaţi, iar aceasta conţine informaţii confidenţiale. În acest caz, serverul trebuie să asigure accesul limitat sau nelimitat la informaţii. Pe acest server vor trebui puse o serie de limite de acces, pentru a identifica utilizatorii care folosesc baza de date. Fiecare calculator (staţie de lucru) nu va fi accesibil decât printr-un nume de utilizator şi o parolă. Serverul conţine informaţii confidenţiale, deci acesta va fi protejat în primul rând fizic.

Politica de securitate

Odată ce informaţiile sunt reperate, trebuie să stabilim o politică de securitate: stabilim cine este autorizat să acceseze serverul şi cine are interdicţie.

Sensibilizarea utilizatorilor

Politica de securitate trebuie prezentată mai întâi utilizatorilor, care trebuie să o înţeleagă şi să respecte regulile stabilite de administratorii de reţea. Regulile fixate de administrator pot viza interzicerea unor acţiuni de tipul consultării lucrărilor unui alt utilizator, citirea de e-mailuri de la persoane necunoscute, acţiuni care pentru unii utilizatori par a nu fi generatoare de riscuri.

Viruşi

Există mai multe tipuri de atacuri folosite de viruşi, deci, fiecare staţie de lucru trebuie să dispună de o *logistică de devirusare actualizată*. Viruşii se transmit în principal pe

dischete, dar şi mail. Fişierele suspecte, care conţin viruşi, sunt de regulă cele cu extensia .com, .exe, dar în egală măsură, documentele pot conţine viruşi de macro.

Securitate necesară, dar nu şi suficientă

Precizăm drept cerinţe minimale în materie de securitate, următoarele:

- autentificarea utilizatorilor printr-un nume şi o parolă;
- interzicerea accesului la informaţiile confidenţiale de pe calculatoarele conectate la reţea, dacă acestea nu sunt folosite în mod curent;
- protejarea fizică a calculatoarelor conţinând date importante (locaţii închise cu cheie);
- controlul accesului logic la informaţiile importante cu ajutorul unui utilizator care vede strict doar datele de care are nevoie pentru realizarea de situaţii finale;
- sensibilizarea utilizatorilor la probleme de securitate;
- instalarea unui antivirus pe fiecare staţie de lucru.

Problema accesului de la distanţă

Datele care circulă pe internet pot fi văzute de toată lumea. Pentru a securiza legătura şi în acelaşi timp să folosim şi reţeaua internet, trebuie să apelăm la VPN (*Virtual Private Network*), unde datele sunt parolate şi nu pot fi citite de persoane neautorizate. În exemplul nostru, staţia de lucru X este conectată direct la reţeaua companiei, fără a utiliza internetul, prin intermediul reţelei private virtuale configurate.

Firewall şi Proxy

După ce s-au stabilit problemele minime de securizare, se impune izolarea reţelei interne de intrări neautorizate. Metoda cea mai cunoscută este folosirea unui firewall şi a unui server proxy. Spre exemplu, la rutere este posibil să se facă filtrarea pachetelor sau schimbul adreselor, pentru o persoană din exterior, care nu are acces nici din interior, nici din exterior, la sistemul organizaţiei. Vom putea analiza datele primite, dar şi interzicerea accesării lor, dacă ele provin de la cineva necunoscut sau nu răspund la cereri interne. Firewall-ul constituie un punct unic de acces prin care se realizează filtrarea transmiterii datelor în reţea (figura 5.7.2).

Un server proxy realizează legătura la nivelul aplicaţiilor, calculatoarele din interior devenind virtuale în exterior. Dacă o persoană din exterior nu poate vedea niciun calculator din reţeaua internă, atunci atacul asupra reţelei este foarte dificil din exterior. Trebuie amintit însă că 80% din atacuri provin din interior.

Logistica detectării sistematice a erorilor

Pirateria utilizează logica testării configuraţiilor pentru a repera sistemele vulnerabile. Această logică permite în mod automat căutarea erorilor configuraţiilor sau vulnerabilitatea sistemului. Dacă acestea sunt folosite înaintea unui atac, atunci va fi mult mai uşor de reparat o eroare de configurare a sistemului dat.

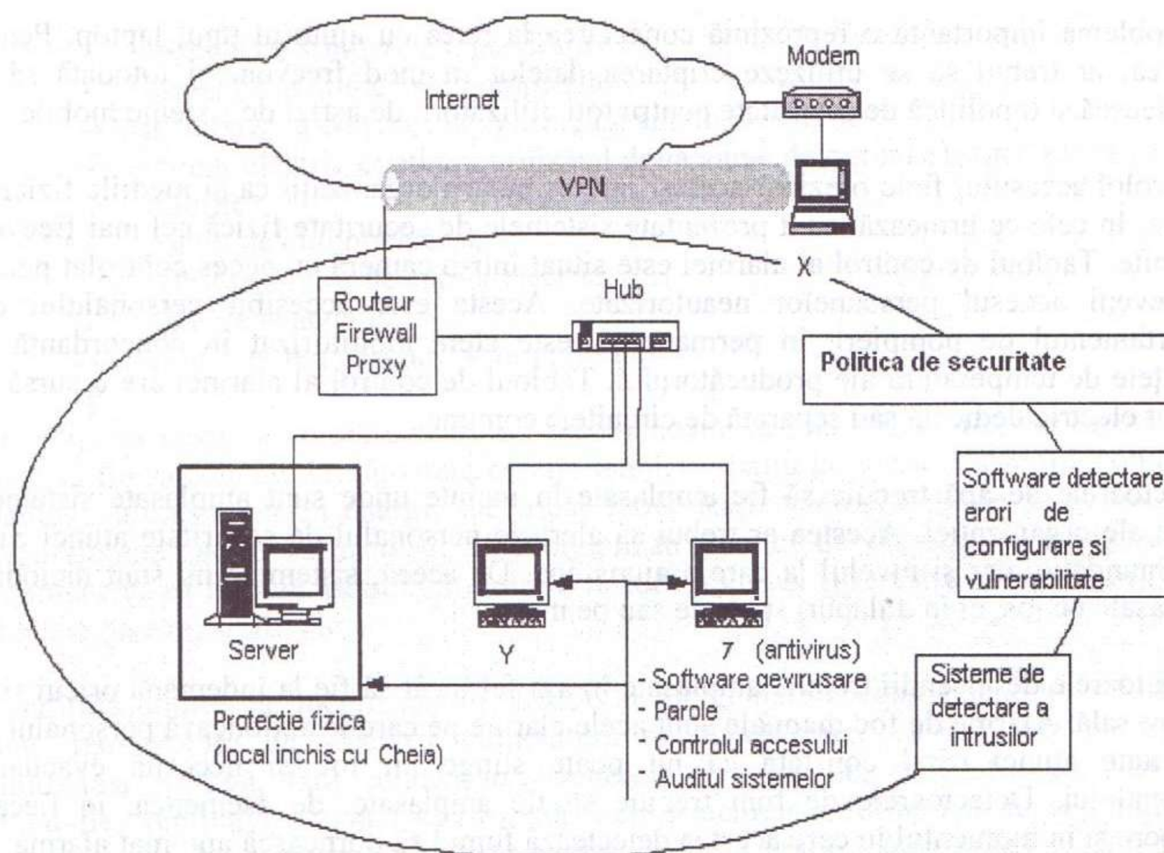


Figura 5.7.2. **Reţea de calculatoare securizată**

Sisteme de detectare a intruşilor

Se poate utiliza o întreagă logistică de detectare a intruşilor. Aşa cum folosim o alarmă la o casă putem detecta un intrus folosind programe de detectare a intruşilor. Acestea nu sunt totdeauna eficace, deoarece intrusul poate fi „mascat" şi deci confundat cu un utilizator al reţelei.

5.8. Controlul accesului fizic şi protecţia echipamentelor electronice de calcul

Principalele pericole pentru un SI din punct de vedere al accesului fizic sunt: intrări neautorizate, vandalism, distrugeri sau furt de echipamente, şantaj, abuz asupra resurselor. Din punct de vedere al unui sistem informatic, trebuie protejate împotriva intruziunilor: mediul de programare, sala unde se găsesc calculatoarele, consola, terminalele, comunicaţiile, sursele de curent electric, liniile telefonice dedicate, LAN, echipamentele portabile, resursele pe care vor fi făcute salvările de siguranţă.

În acest sens, auditul accesului fizic presupune evaluarea pentru: locaţia operatorilor de consolă, camera imprimantelor, sălile unde sunt depozitate/instalate calculatoarele, UPS/generatoare de curent electric, locaţiile echipamentelor de comunicaţie, locaţiile serverelor şi locaţiile de păstrare a copiilor de siguranţă. Următoarele căi fizice de intrare trebuie securizate: uşile destinate intrărilor în incinta cu calculatoare, ferestre, pereţi de sticlă, sisteme de ventilaţie, pereţi falşi, modulari etc.

O problemă importantă o reprezintă conectarea la reţea cu ajutorul unui laptop. Pentru acestea, ar trebui să se utilizeze criptarea datelor în mod frecvent şi totodată să se stabilească şi o politică de securitate pentru toţi utilizatorii de astfel de sisteme mobile.

Controlul accesului fizic prezintă acelaşi interes pentru organizaţii ca şi mediile fizice şi logice. În cele ce urmează, sunt prezentate sistemele de securitate fizică cel mai frecvent întâlnite. Tabloul de control al alarmei este situat într-o cameră cu acces controlat pentru a preveni accesul persoanelor neautorizate. Acesta este accesibil personalului din departamentul de pompieri, în permanenţă, este atent monitorizat în concordanţă cu cerinţele de temperatură ale producătorului. Tabloul de control al alarmei are o sursă de curent electric dedicată sau separată de circuitele comune.

Detectoarele de apă trebuie să fie amplasate în incinte unde sunt amplasate sistemele vitale ale organizaţiei. Acestea ar trebui să alerteze personalul de securitate atunci când este inundaţie, dar şi nivelul la care a ajuns apa. De aceea, sistemele nu sunt niciodată amplasate pe jos, ci în dulapuri speciale sau pe mese.

Stingătoarele de incendii trebuie amplasate în aşa fel încât să fie la îndemâna oricui şi în fiecare sală. Alarme de foc manuale sunt acele alarme pe care le acţionează personalul de securitate atunci când constată că nu poate stinge un foc şi necesită evacuarea personalului. Detectoarele de fum trebuie să fie amplasate, de asemenea, în fiecare încăpere şi în momentul în care acestea detectează fumul să pornească automat alarma. În marile companii, angajaţii sunt instruiţi cu privire la faptul că nu au voie să fumeze în incinta în care este amplasat un sistem electronic de calcul. S-au înregistrat însă şi alarme false, când alarma declanşată de detectorul de fum să fie doar o ţigară fumată într-un loc nepermis. Sistemele de stingere a incendiului sunt de obicei furtunuri conectate la reţeaua de apă, ce pot fi utilizate în caz de incendiu.

Amplasarea strategică a locaţiei calculatoarelor vitale societăţii reduce riscul inundaţiilor, astfel această locaţie ar trebui amplasată la un nivel superior. Inspecţia personalului de la departamentul de pompieri ar trebui să fie făcută periodic, pentru a se asigura faptul că se respectă normele în vigoare. Un element important în protecţia fizică a echipamentelor electronice de calcul îl reprezintă utilizarea materialelor ignifuge în construcţii: tavane, podele, pereţi falşi, dar şi a mobilierului din acea incintă.

Reducerea riscului privind defectarea echipamentelor în timpul unor fluctuaţii de tensiune presupune utilizarea de soluţii alternative pentru sursa de curent electric, cum ar fi UPS, generator de curent electric, butoane de închidere a curentului electric în caz de urgenţă, linii de curent alternativ.

Cel mai important lucru în descoperirea acestor elemente îl constituie întocmirea şi testarea permanentă a unui plan de evacuare în caz de urgenţă şi eliminarea vulnerabilităţilor fizice.

Auditarea controalelor mediului presupune testarea procedurilor privind:

- detectoare de apă şi fum;
- stingătoare manuale de incendiu;

- sisteme de stingere a incendiilor;
- inspecţii periodice ale pompierilor;
- instalarea şi construirea ignifugă a amplasamentelor;
- curent electric continuu utilizând două surse de curent electric (de la centrale diferite);
- panou de curent electric;
- UPS/generator de curent electric;
- plan de evacuare;
- controlul temperaturii şi al umidităţii.

Amenajarea ideală a amplasamentelor, recomandată de specialişti, trebuie făcută astfel încât să fie satisfăcute următoarele cerinţe tehnice: spaţiu de lucru şi stocare, condiţii de mediu, alimentarea cu energie electrică, comunicaţii telefonice şi de date. Spaţiul de lucru trebuie să fie suficient şi bine organizat. Spaţiul de depozitare în siguranţă al echipamentelor trebuie asigurat împotriva furturilor cu uşi şi ferestre cu încuietori, gratii, obloane, la etaj, sigilii etc.

Condiţiile optime de mediu pentru stocare şi funcţionare a echipamentelor informatice sunt: temperatura de stocare, temperatura de funcţionare, variaţia de temperatură, umiditatea relativă, fără condensare, camerele fără igrasie, infiltraţii sau pericol de inundaţie,. ventilaţia naturală sau forţată. Echipamentele informatice nu se amplasează lângă ferestre deschise sau în bătaia soarelui, uşilor cu trafic intens, sobelor, a altor surse de căldură, surse de alimentare cu apă, conducte sau hidranţi, în zone cu vibraţii, în camere unde se stochează sau se lucrează cu substanţe corozive sau volatile.

În jurul echipamentelor trebuie asigurat un perimetru liber necesar pentru ventilaţie. *Nu se vor folosi* echipamentele informatice drept suporţi pentru diferite obiecte, ca recipienţi cu lichide, alimente, flori în ghivece, diferite greutăţi. Pentru stocarea suporturilor de date, a consumabilelor şi a altor subansamble.

Alimentarea cu energie electrică presupune câte două prize cu împământare pentru fiecare calculator, câte o priză cu împământare pentru restul echipamentelor, curent electric de 220 V, 50 Hz, consum maximum 3,5 A, tablou electric cu siguranţe, circuit de alimentare dedicat echipamentelor, legatură la pământ verificată, maximum 5 Ohm, o protecţie la trăznet, prize marcate cu etichete.

Instalaţiile de alimentare cu energie electrică se vor realiza/verifica de un electrician autorizat, care trebuie să fie prezent la instalarea echipamentelor. Conectarea echipamentelor la instalaţii defecte sau improprii poate duce la defectarea acestora şi la pierderea garanţiei. Prizele trebuie dimensionate si alimentate cu tensiune 220 V, 50 Hz la un consum maxim de 3,5 A, cu legătura la pamânt de maximum 5 Ohm. Prizele trebuie să fie în apropierea calculatorului, la mai puţin de 50 cm, deoarece cablul de alimentare trebuie să fie uşor accesibil pentru deconectare în caz de avarie sau dezastru natural. Se recomandă ca prizele să fie instalate pe pereţi ignifugi la 30 cm de sol. Tabloul electric cu siguranţe trebuie verificat, asigurându-se un circuit dedicat echipamentelor informatice. Sursele neînteruptibile de tensiune trebuie instalate şi verificate de personal autorizat. În prizele pentru echipamente informatice ***nu se alimentează***: reşouri, încălzitoare,

ventilatoare, aspiratoare, frigidere, prelungitoare cu prize multiple etc. Prizele de alimentare şi de date se vor eticheta cu CALCULATOR, DATE, TELEFON DIRECT etc. Pentru echipamentele critice (server, ruter, modem) se vor pune etichete cu NU DECONECTATI pe prize şi pe butonul de pornit/oprit. Utilizarea unor instalaţii electrice defecte sau necorespunzătoare conduce la pierderea garanţiei echipamentelor informatice.

5.9. Auditul securităţii SI

Auditul securităţii SI implică auditul accesului fizic şi logic, utilizarea unor tehnici pentru testarea securităţii, precum şi utilizarea tehnicilor de investigare. Pentru aceasta, se parcurg următoarele etape:
- reanalizarea politicilor, procedurilor şi standardelor;
- politici de securitare pentru accesul fizic;
- politici de securitare pentru accesul logic;
- conştientizarea şi formarea permanentă a utilizatorilor privind politicile de securitate;
- stabilirea proprietarilor şi utilizatorilor de date;
- date aflate în custodie;
- administrator de securitate;
- utilizatori noi şi accesul foştilor angajaţi;
- proceduri de autorizare a accesului documentate;
- securitatea de bază ce urmăreşte inventarierea mediului, antivirusul, parole de acces, copii de siguranţă (*backup*), adresarea vulnerabilităţilor, minimizarea serviciilor oferite de sistem, actualizarea sistemului (*patching*), personalul IT;
- accesul standard.

Auditul accesului logic presupune:
- determinarea riscurilor de securitate privind procesarea tranzacţiilor;
- evaluarea controalelor privind căile de acces în sistem;
- evaluarea mediului de control pentru a determina dacă obiectivele controlului sunt atinse de rezultatele testării;
- evaluarea mediului de securitate prin revizuirea politicilor, practicilor şi procedurilor.

Auditul accesului logic presupune în primul rând familiarizarea cu mediul IT pentru a obţine o situaţie clară a securităţii mediului şi evaluarea riscurilor. Un element important îl reprezintă documentarea privind căile de acces, ceea ce se concretizează într-un drum logic al unui utilizator la informaţii. Pentru a controla accesul la componente ale sistemului, sunt ceruţi, adesea, specialişti în domeniu. Aceştia sunt o sursă valoroasă pentru un auditor, în sensul că pot furniza date privind securitatea sistemului. În acest sens, auditorul va cere un interviu cu aceştia şi va stabili vulnerabilitatea politicilor manageriale, securitatea logică şi confidenţialitatea. Se vor avea în vedere şi rapoartele de analiză ale controlului accesului software şi aplicaţiile de analiză ale operaţiilor manuale de sistem.

Auditorul poate utiliza tehnici diferite de testare a securităţii. Unele dintre aceste metode sunt:
- chei şi carduri;
- identificarea terminalului;
- identificarea şi autentificarea utilizatorilor;
- controlul asupra resurselor;
- intrarea în sesiunea de lucru şi raportarea accesului neautorizat;
- urmărirea accesării neautorizate;

- securitatea necontrolată şi controalele de compensare;
- analiza controalelor de acces şi administrarea parolelor.

Investigarea tehnicilor include investigarea protecţiei probelor, obţinerea custodiei, crimei în reţele de calculatoare.

Auditarea securităţii infrastructurii reţelei

Controalele privind auditarea securităţii infrastructurii reţelei presupun verificarea de către auditor a identificării arhitecturii reţelei, determinarea aplicării politicilor de securitate, standarde şi proceduri, identificarea personalului responsabil cu securitatea reţelei, reanalizarea procedurilor administrării reţelei, în cazul în care au apărut noi vulnerabilităţi. În acest sens, auditarea implică auditarea accesului de la distanţă, auditarea punctelor în care interacţionează reţeaua de calculatoare cu reţeaua internet.

Combinarea procedurilor sunt numite teste de penetrare sau teste de intruziune. Aceste teste sunt de mai multe feluri, depinzând de scopul, obiectivul şi natura testului: teste externe (atacuri şi controale provenite din exterior, cum ar fi internetul), teste interne (din acelaşi perimetru), teste „oarbe" (testul este limitat sau nu prezintă cunoştinţe despre sistem) şi teste dublu „oarbe", teste cu o destinaţie anume.

Etapele testelor de penetrare sunt: planificarea, descoperirea, atacul şi raportarea. În testarea de penetrare sunt luate în calcul analiza evaluării reţelei, evaluarea reţelelor LAN, dezvoltarea şi autorizarea schimbărilor în reţea, precum şi schimbări neautorizate.

5.10. Test de evaluare a cunoştinţelor

1. Care dintre următoarele afirmaţii furnizează cadrul pentru proiectarea şi dezvoltarea controalelor de acces logic?
   a. politica de securitate a sistemelor informaţionale;
   b. liste de control al accesului;
   c. managementul parolelor;
   d. fişierele de configurare a sistemului.

2. Un intrus (*hacker*) ar putea afla parolele unui sistem fără a utiliza instrumente software specializate prin tehnica:
   a. ingineriei sociale;
   b. urmărire (*snifer*);
   c. uşa din spate (*back door*);
   d. cal troian (*trojan horse*).

3. Un auditor, care face o clasificare independentă a sistemelor (aplicaţiilor), trebuie să considere funcţiile care pot fi executate manual la un cost tolerabil într-o perioadă de timp extinsă ca fiind:
   a. critice;
   b. vitale;
   c. sensibile;
   d. necritice.

4. Primul motiv pentru utilizarea semnăturii digitale este asigurarea:
   a. confidenţialităţii;
   b. integrităţii;
   c. disponibilităţii;
   d. oportunităţii.

5. În modelul ISO/ OSI, care dintre următoarele niveluri este primul pentru a asigura securitatea utilizatorilor aplicaţiei:
   a. nivelul sesiune;
   b. nivelul transport;
   c. nivelul reţea;
   d. nivelul prezentare.

6. Care dintre următoarele afirmaţii este cea mai sigură şi economică metodă pentru conectarea reţelei private a unei companii de dimensiune mică sau medie la internet?
   a. reţea virtuală privată;
   b. linii dedicate;
   c. linii închiriate;
   d. ISDN (*Integrated Services Digital Network*).

7. Primul scop în certificarea unui site web este:
   a. autentificarea site-ului web ce va fi navigat;
   b. autentificarea utilizatorului care navighează cu ajutorul acestui site;
   c. prevenirea navigării site-ului web de către hackeri;
   d. acelaşi rezultat ca la un certificat digital.

8. Când se face o evaluare de detaliu a unei reţele şi a controalelor de acces, auditorul IS trebuie mai întâi să efectueze:
   a. determinarea punctelor de intrare;
   b. evaluarea accesului autorizat al utilizatorilor;
   c. evaluarea identificării şi autorizării utilizatorilor;
   d. evaluarea configurării serverului.

9. Care dintre următoarele mesaje furnizează cea mai puternică dovadă că o acţiune specificată s-a întâmplat?
   a. dovada trimiterii;
   b. nonrepudierea;
   c. dovada ascultării;
   d. autentificarea originii mesajului.

10. Un producător a cumpărat materiale printr-o aplicaţie de e-comerţ. Care dintre următoarele afirmaţii trebuie să fie sprijin pentru producător pentru a dovedi că tranzacţiile au fost făcute?
   a. reputaţia;
   b. autentificarea;
   c. criptarea;
   d. nonrepudierea.

Capitolul 6

Sisteme de criptare

Capitolul 6

Sisteme de criptare

Criptarea este procesul de transformare a unui mesaj dintr-o formă în care poate fi citit, denumit în termeni criptografici „text clar", într-o formă codificată, „text criptat" sau „text cifrat", care nu poate fi înţeles fără revenirea la textul iniţial. Operaţia de transformare inversă, din „text criptat" în „text clar" poartă numele de ***decriptare***.

Criptarea, respectiv decriptarea, se realizează printr-o funcţie matematică şi o *cheie*. Termenul *cheie* se referă la o informaţie, de regulă în formă binară, de o anumită lungime, care este folosită împreună cu un algoritm criptografic, pentru criptare şi/sau decriptare. În cazul criptării, cheia afectează modul în care datele sunt transformate. În cazul decriptări doar prin folosirea unei chei corespunzătoare se pot recupera datele originale. Trebuie menţionat faptul că prin criptare nu putem preveni pierderea datelor.

Criptarea în general se utilizează pentru:

- protejarea datelor în tranzit prin reţelele de calculatoare împotriva interceptărilor şi manipulărilor neautorizate;
- protejarea datelor stocate pe calculatoare împotriva vizualizărilor şi manipulărilor neautorizate;
- detectarea şi prevenirea modificării accidentale sau intenţionate a datelor;
- verificarea autenticităţii tranzacţiilor sau documentelor.

Sistemele criptografice sunt de două tipuri:

- *sisteme criptografice cu chei secrete* (simetrice) - cheia de criptare este aceeaşi cu cheia de decriptare;
- *sisteme criptografice cu chei publice* (asimetrice) - cheia de criptare este diferită de cheia de decriptare (cele două chei sunt dependente).

6.1. Criptografia cu cheie secretă

Cea mai folosită metodă de criptare este cea cu ***cheie secretă***, în care ambele părţi implicate în comunicare deţin o singură cheie, care trebuie ţinută secretă. Această metodă asigură confidenţialitatea deoarece o a treia persoană, teoretic, nu poate interpreta mesajul criptat.

Totuşi, apar o serie de probleme, de exemplu: cum se poate transmite cheia secretă în siguranţă între cele două părţi? Mai mult, pentru fiecare pereche expeditor-destinatar este nevoie de o cheie. De exemplu, dacă cineva are nevoie să trimită mesaje către alte n persoane, trebuie să folosească o altă cheie pentru fiecare persoană în parte, deoarece, dacă foloseşte aceeaşi cheie de două ori, va exista o a treia persoană care cunoaşte cheia de criptare a mesajului. Cu cât creşte numărul persoanelor care iau parte la comunicaţie, cu atât creşte complexitatea mecanismului pentru managementul cheilor de criptare.

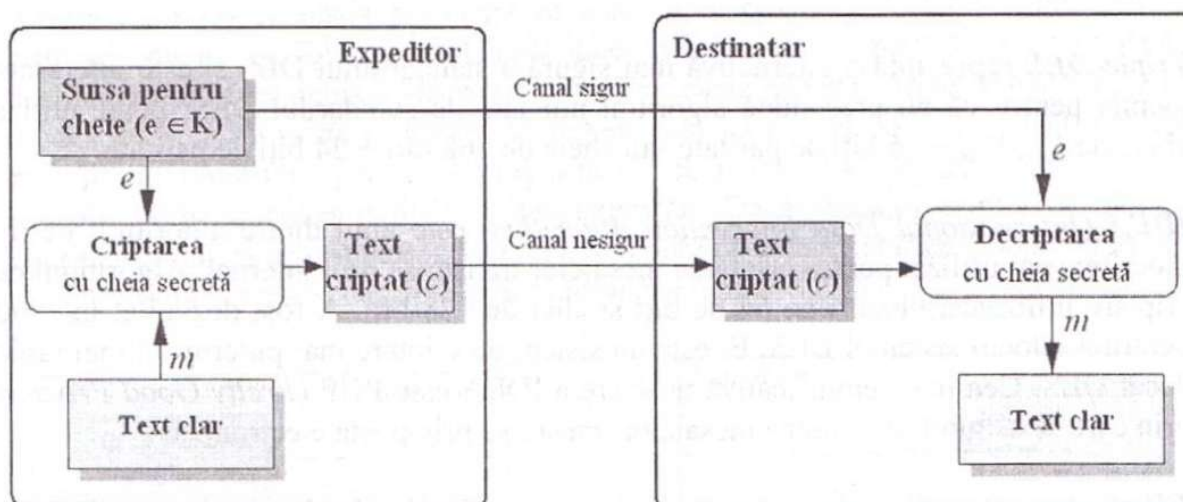


Figura 6.1.1. **Criptarea cu cheie secretă**

Pentru codificarea cu cheie secretă există două tipuri de algoritmi: *algoritmi bloc* – care operează asupra textului iniţial la nivel de blocuri de biţi (folosit în mod frecvent) şi *algoritmi de tip stream* - care operează asupra unui bit (sau byte) al textului original la un moment dat. Algoritmii de criptarea bloc cu cheie simetrică sunt elemente importante în multe sisteme criptografice.

Cel mai utilizat sistem criptografic cu cheie simetrică este **DES** (*Data Encryption Standard*). Standardul de criptare DES a fost realizat printr-un proiect IBM, demarat în anul 1970, care prevedea dezvoltarea unui algoritm care să nu poată fi spart, nici de cele mai rapide calculatoare ale timpului respectiv. Normele FIPS (*Federal Information Processing Standards*) impuneau ca algoritmul să fie aplicat pentru criptarea informaţiilor care nu erau considerate secret de stat. Deşi algoritmul este complex, este foarte uşor de implementat hardware, iar din punct de vedere software există foarte multe soluţii. În 1977, DES a fost aprobat ca standard pentru tehnica de criptare/decriptare de către Oficiul Naţional de Standardizare al SUA (*US National Bureau of Standard – NBS*), predecesorul lui NIST (*National Institute of Standards and Technology*).

- DES este bazat pe un algoritm de tip bloc, care separă textul clar în blocuri de 64 de biţi şi foloseşte o cheie de 56 biţi generată aleatoriu, exprimată ca un număr pe 64 biţi (cei 56 biţi pentru cheie + 8 biţi pentru paritate). Orice număr reprezentat pe 56 de biţi poate fi utilizat ca o cheie; există 2^{56} posibile chei.

DES nu este considerată o soluţie de criptare puternică, deoarece cheia corectă poate fi identificată printr-un atac de tip „forţă brută". Având în vedere că spaţiul cheilor este redus, un calculator puternic nu are nevoie de prea mult timp pentru încercarea tuturor cheilor posibile.

Triple-DES reprezintă o alternativă mai sigură a standardului DES şi este interesant tocmai pentru că nu presupune algoritmi noi faţă de standardul DES; poate utiliza cheie de 112 biţi + 16 biţi de paritate sau cheie de 168 biţi + 24 biţi de paritate.

IDEA (*International Data Encryption Algorithm*) este unul dintre algoritmii de tip bloc frecvent utilizat pentru criptarea mesajelor transmise prin internet. Algoritmul de criptare utilizează blocuri pe 64 de biţi şi chei de 128 biţi. A fost dezvoltat în 1990 pentru a înlocui sistemul DES. El este un sistem de criptare mai puternic şi mai rapid decât DES. Cea mai semnificativă utilizare a IDEA este PGP (*Pretty Good Privacy*) prin care se asigură securitatea mesajelor transmise prin poşta electronică.

FEAL (*Fast Data Encipherment Algorithm*) este o familie de algoritmi care utilizează blocuri pe 64 de biţi şi chei de 64 biţi.

RC2 şi ***RC4***: algoritmi care utilizează chei de criptare variabile, între 40 şi 128 de biţi.

A5 este un exemplu de algoritm de *tip stream* pentru criptarea traficului prin telefoanele celulare care utilizează standardul GSM, folosit pe larg în Europa.

Avantajul sistemelor criptografice cu cheie secretă constă în faptul că atât criptarea, cât şi decriptarea se realizează cu aceeaşi cheie şi transformarea se execută uşor şi repede datorită numărului mic de calcule conţinut în algoritm, comparativ cu metoda criptării cu chei publice. Acesta este motivul pentru care criptografia cu cheie secretă ocupă un rol important în multe protocoale de securitate folosite în internet, cum ar fi protocolul SSL (*Secure Socket Layer*). Dezavantajul major îl reprezintă modul cum poate fi obţinută cheia, pentru a o folosi la criptarea datelor schimbate, de exemplu pentru un mediu de afacere. Managementul cheilor este o altă problemă importantă în cazul acestor sisteme. În plus, cheia secretă nu poate fi folosită pentru semnarea electronică a documentelor sau mesajelor, deoarece mecanismul este bazat pe o partajare secretă.

6.2. Criptografia cu cheie publică

În anul 1976, W. Diffie şi M. Hellman, cercetători la Universitatea Stanford din California, au pus bazele criptografiei cu cheie publică, care a rezolvat problema legată de transmiterea cheii private între partenerii de comunicaţie în cazul în care se utiliza sistemul criptografic cu cheie secretă. În cadrul sistemului cu cheie publică sau chei asimetrice se utilizează o pereche de chei - *cheia privată* şi *cheia publică*. Cheia folosită pentru criptare este diferită de cheia folosită pentru decriptare. În sistemul criptografic cu cheie publică este necesar ca posesorul cheilor să-şi protejeze cheia privată, în timp ce cheia publică este pusă la dispoziţia celorlalţi. Algoritmul de criptare este în aşa fel conceput încât dacă mesajul este criptat cu cheia publică a destinatarului el va putea fi decriptat numai cu cheia privată corespondentă, deţinută de destinatar şi nu poate fi decriptat cu cheia folosită pentru criptare. Acest principiu este foarte important pentru criptografia cu cheie publică, în care mesajele sunt criptate folosind cheia publică a destinatarului. Dacă mesajul criptat ar putea fi decriptat cu cheia de criptare (care este cheia publică a destinatarului, obţinută în mod public) oricine ar putea decripta şi citi mesajele (figura 6.2.1).

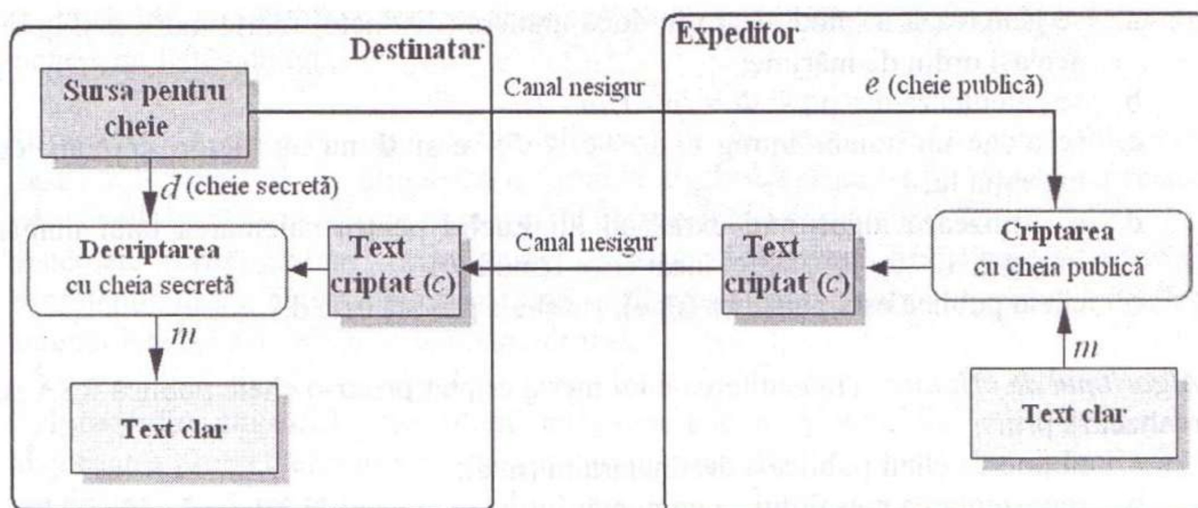


Figura 6.2.1 **Tehnica pentru criptarea cu cheie publică**

Confidenţialitatea datelor este asigurată şi în cazul criptografiei cu cheie publică, o a treia parte nu poate înţelege mesajul criptat. Numai destinatarul poate citi mesajul primit, deoarece doar el deţine cheia privată corespondentă pentru decriptarea mesajului. Totuşi, oricine poate trimite mesaje criptate unui destinatar folosind cheia publică a acestuia, care este accesibilă tuturor. Destinatarul poate citi mesajele, dar nu poate fi sigur că ele provin chiar de la cei care pretind că le-au expediat. Oricine are acces la cheia publică a destinatarului şi o poate folosi în numele altcuiva.

Criptografia cu cheie publică nu o înlocuieşte pe cea cu cheie secretă. De fapt, cele două tehnici se completează, pentru a oferi un nivel ridicat de securitate, fără a diminua viteza şi performanţa.

De reţinut, sistemul criptografic cu cheie publică îmbunătăţeşte nivelul de securitate. Cheile publice sunt distribuite liber, iar utilizatorii nu trebuie să administreze prea multe chei. Utilizatorii au responsabilitatea de a-şi ţine la loc sigur cheia lor privată.

6.2.1. Sistemul criptografic RSA

Unul dintre cele mai utilizate sisteme criptografice cu cheie publică este ***RSA*** (Rivest, Shamir şi Aldeman), lansat în 1977, fiind recunoscut ca având cea mai sigură metodă pentru criptare şi autentificare. Sistemul RSA include câte un algoritm pentru: generare de chei, criptare şi decriptare.

Algoritmul de generare a cheilor. Fiecare entitate creează o cheie publică RSA şi cheia privată corespunzătoare prin parcurgerea etapelor:

a. se generează în mod aleatoriu două numere (distincte) foarte mari, p şi q, de acelaşi ordin de mărime;
b. se calculează n = pq şi $\Phi = (p - 1)(q - 1)$;
c. se alege un număr întreg *e*, $1 < e < \Phi$; e şi Φ nu au factori comuni, cu excepţia lui 1;
d. se utilizează algoritmul extins al lui Euclid pentru calcularea unui număr întreg d, $1 < d < \Phi$, astfel încât $ed \equiv 1(\text{mod } \Phi)$;
e. cheia publică este perechea (n, e), iar cheia privată este d.

Algoritmul de criptare. Transmiterea unui mesaj criptat printr-o cheie publică RSA se realizează prin:
a. obţinerea cheii publice a destinatarului (n, e);
b. reprezentarea mesajului ca un număr întreg m cuprins în intervalul [0, n-1];
c. se calculează $c = m^e \text{ mod } n$;
d. se emite textul criptat c la destinaţie.

Algoritmul de decriptare. Pentru obţinerea numărului întreg m din c, la destinaţie se calculează:

$$m = c^d \text{ mod } n,$$

d fiind cheia privată a destinatarului.

Exemplu
Algoritmul de generare chei:
a. se aleg numerele prime p = 2.357, q = 2.551;
b. se calculează n = pq = 6.012.707 şi $\Phi = (p - 1)(q - 1) = 6.007.800$;

c. se alege e = 3.674.911;
d. utilizând algoritmul lui Euclid extins, se găseşte d = 422.191 astfel că $ed \equiv 1(\text{mod } \Phi)$.
e. cheia publică va fi perechea (n = 6.012.707; e = 3.674.911), iar cheia privată este d = 422.191.

Algoritmul de criptare. Pentru transmiterea mesajului m = 5.234.673, prin algoritmul de criptare se calculează:

$c = m^e \text{ mod } n = 5.234.673^{3674911} \text{ mod } 6.012.707 = 3.650.502;$

şi se emite către destinatar.

Algoritmul de decriptare. Pentru decriptarea mesajului recepţionat se va calcula:

$c^d \text{ mod } n = 3.650.502^{422191} \text{ mod } 6.012.707 = 5.234.673.$

6.2.2. Criptografia prin curbe eliptice

O variantă şi o formă mai eficientă a criptografiei cu cheie publică este criptografia bazată pe curbe eliptice. De exemplu, criptarea prin curbe eliptice care utilizează o cheie de 160 de biţi oferă aceeaşi securitate ca un sistem bazat pe RSA care foloseşte o cheie de 1.024 de biţi.

Sistemele de criptare prin curbe eliptice au la bază rezolvarea problemelor logaritmilor discreţi. Se utilizează o formulă algebrică pentru a se determina relaţia între cheile publice şi private în universul creat printr-o curbă eliptică.
Sistemele criptografice prin curbe eliptice realizează următoarele servicii: confidenţialitatea, autentificarea părţilor implicate în comunicaţie, integritatea datelor, nerepudierea şi schimbul de chei autentificat.

Criptografia cuantică este următoarea generaţie a criptografiei care va rezolva majoritatea problemelor asociate sistemelor criptografice existente (dar, în mod sigur, vor apărea probleme noi).

6.2.3. AES (*Advanced Encryption Standard*)

Descoperirile recente în domeniul criptografiei, combinate cu creşterea, din ce în ce mai mare, a puterii de procesare a unităţilor centrale, au determinat ca algoritmul DES să fie pus sub semnul întrebării.

In 1997, NIST a anunţat intenţia de a dezvolta standardul AES, prin care să înlocuiască DES. S-a dorit ca AES să reprezinte un standard pentru prelucrarea informaţiilor şi să includă un algoritm de criptare pentru protejarea informaţiilor senzitive. Criteriile stabilite pentru AES presupuneau un algoritm care să fie disponibil publicului larg din întreaga lume, un cifru pe blocuri de date, care să suporte blocuri de minimum 128 de biţi şi chei de lungime de 128, 192 şi 256 de biţi.

În august 1998, NIST a anunţat existenţa a 15 algoritmi candidaţi pentru AES, din care a selectat numai cinci: MARS, RC6, Rijndael, Serpent şi Twofish.

În urma unei analize complexe, pe 2 octombrie 2000, NIST a anunţat că a fost selectată propunerea *Rijndael*, ca algoritm pentru standardul AES. Algoritmul Rijndael a fost dezvoltat de dr. Joan Daemen şi dr. Vincent Rijmen. Rijndael este un cifru simetric cu lungimea cheii şi a blocului de date variabile. Pentru AES lungimea blocului de date poate fi fixată la 128 de biţi şi dimensiunea cheii ar putea avea trei valori diferite: 128, 192 sau 256 de biţi. Există trei versiuni diferite ale standardului AES: AES-128, AES-192 şi AES-256. Criptarea se bazează pe operaţii succesive de rotunjire. Fiecare rotunjire are o cheie proprie de 128 de biţi, rezultatul unei operaţii de rotunjire reprezintă intrarea pentru următoarea. Cheile pot fi precalculate sau generate. Datorită acestei structuri regulate, algoritmul prezintă o creştere a vitezei de execuţie, în raport cu DES, şi poate fi implementat în mod eficient atât prin hardware, cât şi prin software. Pentru decriptare, se aplică funcţiile inverse operaţiilor de rotunjire. Performanţele de calcul ale implementărilor software sunt diferite în faza de criptare faţă de cele de la decriptare; deoarece operaţiile de decriptare sunt mai complexe. De remarcat, algoritmul poate fi implementat şi pe dispozitivele care rulează pe 8 biţi, aşa cum sunt cardurile inteligente.

6.3. Semnătura digitală

Una dintre cele mai importante contribuţii oferite prin criptografia cu cheie publică este *semnătura digitală*. Primul standard internaţional pentru semnătura digitală (ISO/IEC 9796) a fost adoptat în 1991. El are la bază schema cu cheie publică RSA. În 1994, guvernul SUA a adoptat DSS (*Digital Signature Standard*), un mecanism bazat pe schema cu cheie publică ElGamal.

Ce reprezintă semnătura digitală? Uneori, cheia privată a expeditorului poate fi utilizată pentru criptare. Destinatarul va folosi atunci cheia publică a expeditorului pentru a decripta şi citi mesajul. În acest caz destinatarul poate fi sigur că mesajul provine într-adevăr de la expeditor, deoarece doar acesta deţine cheia privată. Când este folosită într-un asemenea mod, noţiunea de criptare se înlocuieşte cu cea de *semnare*. Expeditorul nu poate nega faptul că a trimis un mesaj, dacă acesta a fost criptat cu cheia lui privată. În acest fel, pe lângă confidenţialitatea datelor, se mai asigură autentificarea şi nerepudierea. Cel mai mare dezavantaj al sistemului criptografic cu cheie publică îl reprezintă timpul mare de criptare şi decriptare.

Din prezentările anterioare reiese că sistemele criptografice bazate pe cheie publică pot fi utilizate pentru garantarea:

- *confidenţialităţii* - criptarea mesajului transmis se realizează cu cheia publică a destinatarului;

- *autentificării* - criptarea mesajului transmis se realizează cu cheia secretă a celui care expediază mesajul.

Ambele metode implică aplicarea algoritmului de criptare întregului mesaj, care la rândul său necesită un proces intens de calcul. Dacă se are în vedere că unele mesaje pot fi foarte mari, atunci timpul alocat calculelor va fi considerabil.

Soluțiile disponibile elimină acest neajuns. Dacă vom considera notațiile:
- M este setul mesajelor care vor fi semnate;
- S este setul elementelor denumite semnături, un şir binar de lungime fixă;
- S_A este o transformare de la setul de mesaje M la setul de semnături S, denumită *transformarea de semnare* (*signing transformation*) pentru entitatea A. Transformarea S_A este păstrată secretă de A şi va fi utilizată pentru crearea semnăturilor mesajelor din M;
- V_A este transformarea de la setul M x S la setul {*adevărat, fals*}. V_A este denumită *transformarea de verificare* pentru semnătura entității A, care este publică, şi este utilizată de alte entități pentru verificarea semnăturilor create de A.

Procedura de semnare

Entitatea A care emite (cel care semnează) creează o semnătură pentru mesajul m $\in$ M prin:
1. se calculează $s = S_A(m)$;
2. se transmite perechea (m,s); s poartă numele de *semnătură* pentru mesajul m.

Procedura de verificare

Pentru a verifica dacă semnătura s a mesajului m a fost creată de A, entitatea B (cel care verifică) urmează etapele:
1. obține funcția de verificare V_A a lui A;
2. calculează $u = V_A(m,s)$;
3. acceptă semnătura creată de A dacă u = *adevărat* şi elimină semnătura dacă u = *fals*.

Semnătura digitală asigură **integritatea** datelor, **autentificarea**, şi **nerepudierea** mesajelor.

Funcțiile de dispersie (*hash functions*) au un rol fundamental în sistemele criptografice moderne, fiind un instrument pentru crearea rezumatului unui mesaj. Funcțiile *hash* au ca intrare un mesaj de lungime variabilă şi generează un mesaj de lungime fixă, referit ca *valoare hash, cod hash, rezultat hash* sau simplu *hash*. În mod obişnuit, valoarea *hash* se reprezintă pe 128 sau 160 de cifre binare.

Când o *funcţie hash* utilizează o cheie privată ca un parametru de intrare secundar, ieşirea va depinde atât de mesaj, cât şi de cheie, şi poartă numele de *codul de autentificare a mesajului* (MAC - *Message Authentification Code*).

Un algoritm pentru obţinerea codului de autentificare a mesajului este o familie de funcţii de dispersie h_k parametrizate printr-o cheie secretă k, având următoarele proprietăţi:

- *uşor de calculat* - pentru o funcţie cunoscută h_k, fiind dată valoarea k şi intrarea m, $h_k(m)$ este uşor de calculat; rezultatul poartă numele de *valoare MAC* sau *MAC*;
- *comprimarea* – prin aplicarea funcţiei h_k unei intrări m de lungime finită arbitrară la ieşire $h_k(m)$se va obţine o lungime fixă n; executând aceeaşi *funcţie hash* asupra aceluiaşi mesaj se va obţine acelaşi rezultat;
- *rezistenţa la calcul* – fiind date zero sau mai multe perechi text-MAC $(m_i, h_k(m_i))$ este imposibil să se calculeze o pereche $(m, h_k(m))$ pentru o nouă intrare $m \neq m_i$; nu este o operaţie previzibilă - aceasta înseamnă că o modificare oricât de mică a mesajului va avea un efect de dimensiune mare şi neprevizibil asupra valorii *hash*;

Cele mai utilizate scheme pentru calcularea rezumatelor de mesaje sunt:

- ***MD2*** (*Message Digest*) – una dintre primele funcţii hash, propusă în 1988 de Rivest; algoritmul de dispersie generează o valoare hash de 128 de biţi;
- ***MD4*** – a fost proiectat special pentru implementările software în calculatoarele care lucrează pe 32 de biţi; valoarea hash este de 128 biţi;
- ***MD5*** – schemă de dispersie standard în domeniu. Calcularea rezumatului unui mesaj se face în cinci etape. Mesajul iniţial este completat până la un multiplu de 512 biţi. Fiecare din aceste blocuri de 512 de biţi este trecut printr-un proces care cuprinde patru runde, în fiecare rundă se execută un set de operaţii, rezultând o valoare care reprezintă parametrul de intrare pentru procesarea următorului bloc de 512 de biţi. Rezultatul hash este o valoare de 128 de biţi determinată în urma procesării ultimului bloc de 512 de biţi.
- ***SHA1*** (*Secure Hash Algorithm*) – se bazează în principal pe studiul depus în realizarea algoritmilor din seria MD. Mesajul iniţial este completat până la un multiplu de 512 biţi, precum MD5, şi apoi este trecut printr-un proces de patru runde, a 20 de operaţii fiecare. Valoarea transferată de la o rundă la alta este de 160 de biţi, ceea ce înseamnă că şi valoarea *hash* este tot de 160 de biţi.

Dacă autentificarea mesajului recepţionat este principalul obiectiv, atunci o rezolvare ar fi:

- se va genera mai întâi un rezumat al mesajului, prin folosirea unei funcţii de dispersie;
- se va cripta rezumatul cu cheia privată a expeditorului;

- mesajul criptat rezultat reprezintă *semnătura digitală* şi se poate ataşa mesajului în clar.

Aşadar, rezumatul mesajului calculat cu funcţia *hash* poate fi considerat o amprentă a mesajului original. Semnătura digitală este adăugată mesajului original (în clar) şi împreună se trimit destinatarului.

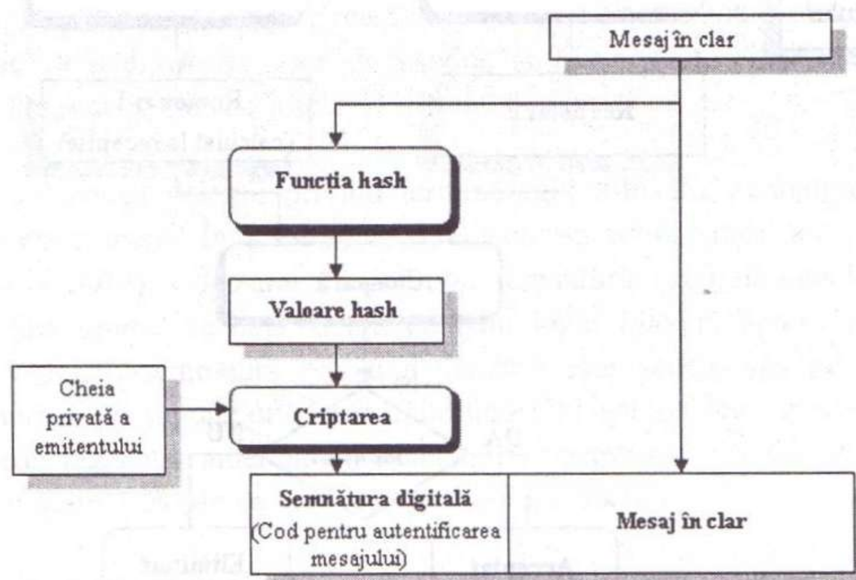


Figura 6.3.1 **Generarea codului pentru autentificarea mesajului**

La recepţie, semnătura digitală se va separa de mesajul în clar. Cum poate fi sigur destinatarul că mesajul este de la adevăratul expeditor sau el nu a fost alterat pe parcurs? Pentru a se convinge, este necesară operaţia de verificare, prin parcurgerea următorilor paşi:

1. se aplică funcţia *hash* (aceeaşi ca la emisie) mesajului în clar recepţionat şi se obţine un prim rezumat;
2. se decriptează semnătura digitală recepţionată cu cheia publică a expeditorului, obţinându-se cel de-al doilea rezumat al mesajului;
3. se compară cele două rezumate obţinute la punctele 1 şi 2. Dacă rezumatele sunt identice, se poate declara că mesajul nu a fost alterat şi provine de la adevăratul expeditor. În caz contrar, fie conţinutul mesajului a fost modificat prin canalul de comunicaţie sau semnătura este falsă.

Aşadar, aplicând o semnătură digitală unui mesaj, destinatarul se va asigura că expeditorul este într-adevăr cel care se pretinde a fi şi că mesajul nu a fost alterat de-a lungul canalului de comunicaţie, ceea ce înseamnă că se garantează autentificarea şi nerepudierea expeditorului şi păstrarea integrităţii datelor.

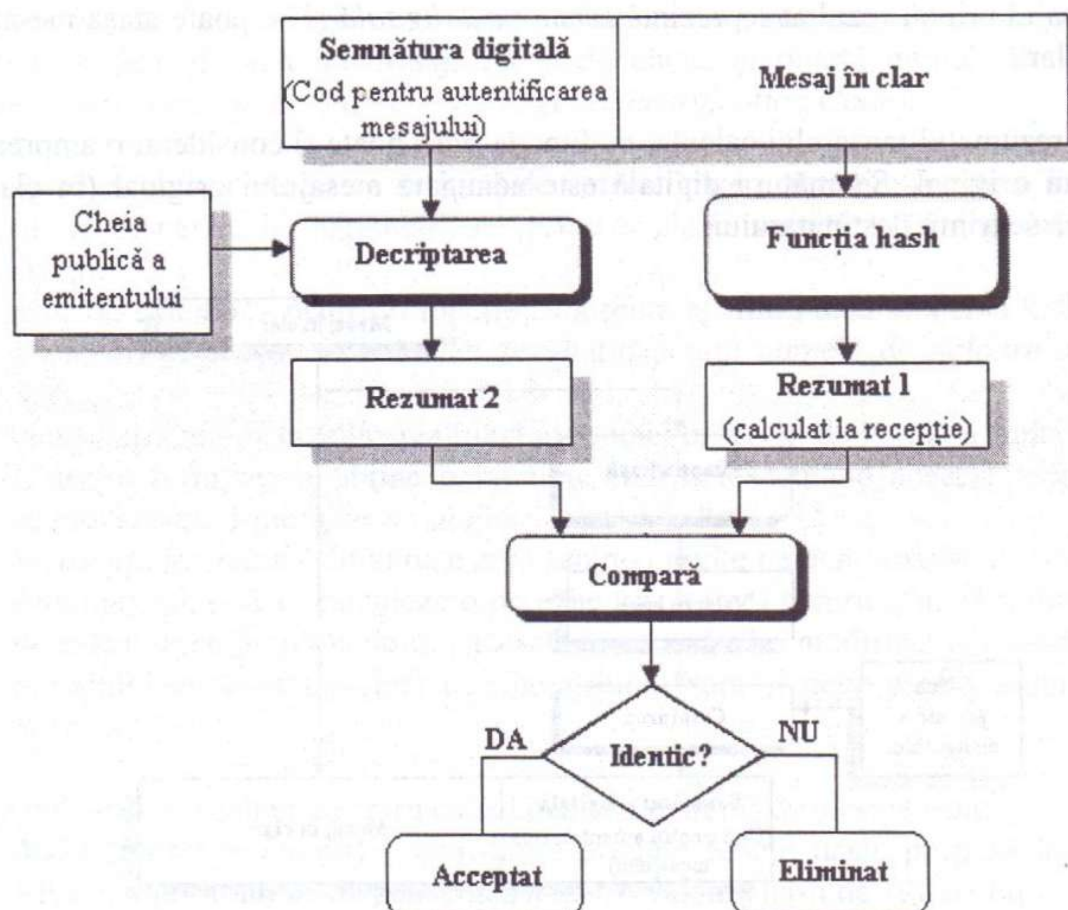


Figura 6.3.2. **Verificarea la recepţie a integrităţii şi autenticităţii**

Totuşi, scenariul prezentat este doar un caz ideal. O presupunere a fost făcută: la pasul 2 cheia publică a expeditorului este folosită pentru decriptare. Dar poate fi această cheie sigură? Această cheie poate să nu aparţină adevăratului expeditor. Cineva poate să înşele mecanismul schimbând mesajul în prima fază, apoi oferind o cheie publică falsă. Cele două rezumate ale mesajelor generate la paşii 1 şi 2 vor fi la fel, dar mesajul şi expeditorul nu vor mai fi de încredere. Schema de securitate şi ierarhia de încredere trebuie adăugate semnăturii digitale pentru a îmbunătăţi modelul în ansamblu.

Dacă se doreşte confidenţialitatea mesajului transmis, este necesară criptarea lui. Pentru a obţine acest lucru, emitentul va aplica asupra mesajului un algoritm rapid de criptare simetrică, utilizând o cheie oarecare. Cheia folosită pentru criptarea simetrică va fi şi ea transmisă, fiind inclusă în mesaj după ce a fost criptată cu cheia publică a destinatarului.

La recepția mesajului, destinatarul va separa cele două zone: cheie criptată şi mesaj criptat. Apoi, folosind cheia sa secretă, va decripta cheia simetrică. În continuare, aplicând mesajului criptat recepționat acelaşi algoritm simetric ca la emisie, folosind cheia identificată anterior, va avea acces la textul în clar.

Pentru a înlocui semnătura olografă cu ce electronică pe documentele oficiale trebuie ca oamenii să aibă încredere în cea de-a doua şi să existe reglementările necesare implementării acesteia. Pentru aceasta, semnătura electronică trebuie să satisfacă următoarele cerințe: să fie uşor de produs şi recunoscut, dificil de falsificat şi tehnologia folosită să fie clar înțeleasă de toată lumea.

Există de asemenea discuții privind terminologia folosită: semnătură digitală sau semnătură electronică? În acest sens, Asociația Baroului American (*American Bar Association – ABA*) a declarat că definiția semnăturii (digitală sau electronică) ar trebui să țină seama de dependența de tehnologia folosită pentru implementarea acesteia. Astfel, o semnătură este digitală dacă este dependentă de tehnologia de implementare şi presupune utilizarea unor algoritmi criptografici cu chei publice (aşa cum prevede legislația americană). Semnătura electronică este neutră din punct de vedere tehnologic (abordarea la nivelul Uniunii Europene).

Abordarea dependentă de tehnologie (semnătura digitală) are avantajul că legea poate fi elaborată astfel încât să reflecte exact capabilitățile şi limitările tehnologiei respective, dar are şi dezavantajul că limitează libera circulație a produselor şi serviciilor bazate pe tehnologii diferite având un nivel de securitate echivalent sau mai bun. Semnătura electronică poate utiliza atât tehnologia bazată pe criptografia cu chei publice, cât şi alte tehnologii cum ar fi ceea biometrică. Singura tehnologie disponibilă în momentul de față, care satisface cerințele ca o semnătură electronică să fie echivalentă din punct de vedere legal cu semnătura olografă (să fie admisă ca probă în justiție) este cea bazată pe algoritmi criptografici cu chei publice, certificate digitale şi infrastructura de chei publice.

În data de 13 decembrie 1999, Parlamentul şi Consiliul Europei a aprobat Directiva 1999/93/EC privind semnătura electronică, care are ca scop crearea unui cadru uniform pentru toate statele membre în privința adoptării până în luna iulie 2001 a legilor naționale în domeniu.

În România, pe baza Directivei 1999/93/EC, în luna iulie 2001 a fost adoptată Legea nr. 455 privind semnătura electronică, iar în luna decembrie 2001 au fost elaborate Normele metodologice privind aplicarea legii semnăturii electronice.

6.4. Infrastructura de chei publice

Dacă o persoană doreşte să emită mesaje sau documente electronice şi le semnează printr-o semnătură electronică, utilizând un sistem criptografic cu cheie publică, cum se va face distribuţia cheii publice într-un mod securizat? Dacă cheia publică este distribuită electronic, va putea fi interceptată şi schimbată. Pentru a preveni astfel de situaţii este necesar un cadru de lucru, prin care să se stabilească modul de generare, întreţinere şi revocare a certificatelor de chei publice de către o terţă parte. Acest cadru de lucru este cunoscut ca infrastructura de chei publice (*Public Key Infrastructure* – PKI).

Infrastructura de chei publice oferă un cadru tehnic (incluzând protocoale, servicii şi standarde) pentru a sprijini realizarea de aplicaţii care să îndeplinească cele cinci proprietăţi ale securităţii: **autentificarea entităţilor, confidenţialitatea datelor, integritatea datelor, nerepudierea şi managementul cheilor**.

Un sistem de securitate care încorporează certificate şi criptografia bazată pe chei publice este soluţia pentru problemele de securitate existente în cele mai multe organizaţii. PKI permite utilizatorilor să interacţioneze cu alţi utilizatori şi aplicaţii, să obţină şi să verifice identităţi şi chei prin surse de încredere. Implementările actuale ale PKI variază în concordanţă cu cerinţele specifice. Elementele fundamentale ale unei infrastructuri de chei publice sunt:

- *certificatele digitale* reprezintă o colecţie de date în format electronic;
- *Autoritatea de certificare* (*Certification Authority* – CA): are rolul de a emite şi revoca certificate digitale;
- *Autoritatea de înregistrare* (*Registration Authority* – RA): are rolul de a valida cererile de obţinere a certificatelor şi identitatea entităţilor finale;
- *depozite de certificate* (*Repository*): stochează şi distribuie certificatele şi listele de certificate revocate (*Certificate Revocation List* – CRL);
- *entităţile finale* (*End Entity*): reprezintă utilizatori, dispozitive sau aplicaţii software care folosesc certificatele digitale pentru implementarea de servicii de securitate.

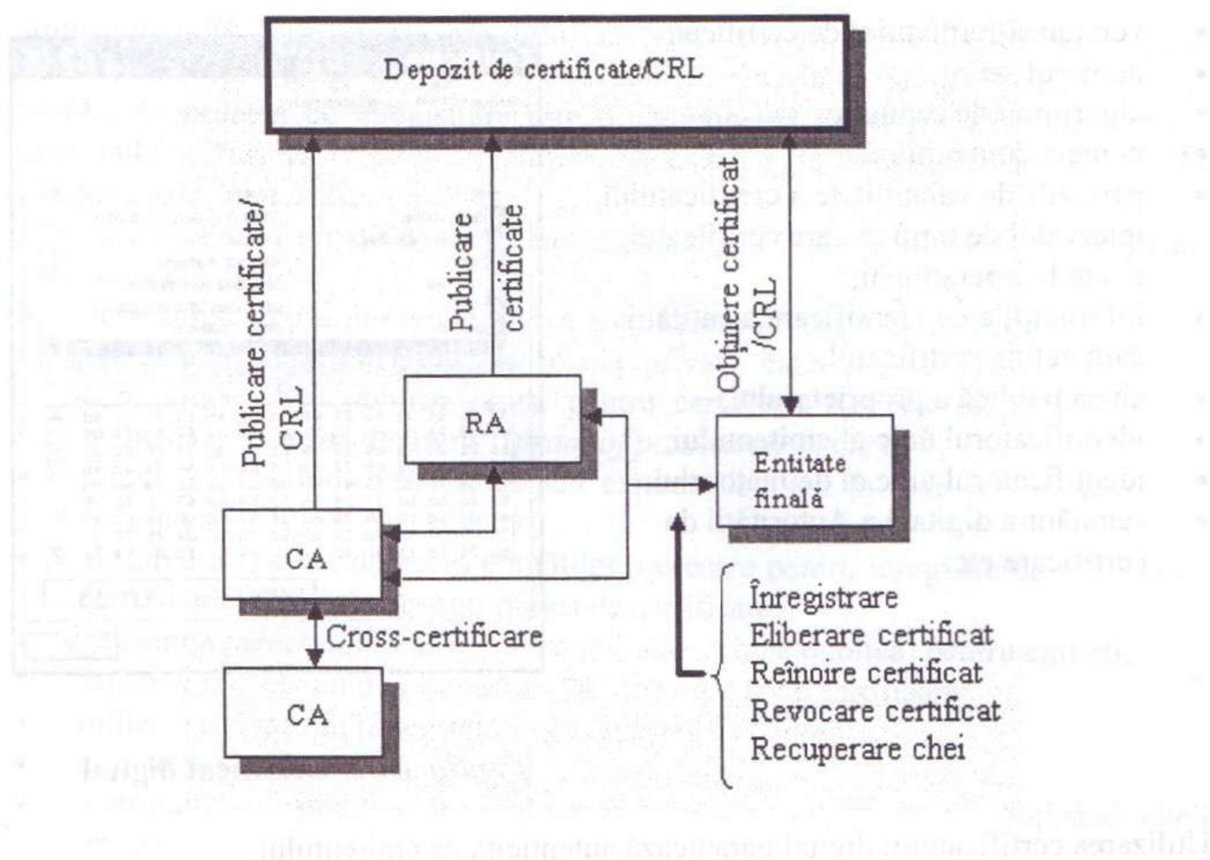


Figura 6.4.1 **Componente PKI**

Certificatul digital este o structură de date care conține o cheie publică și o serie de informații pentru identificarea unică a entității care deține cheia. Rolul certificatelor digitale este de a asocia o cheie publică cu o identitate individuală. Cerificatele digitale sunt documente electronice, semnate digital de o entitate de încredere, aceasta fiind Autoritatea de certificare. Recomandările X.509 definesc formatul certificatelor digitale, care includ următoarele câmpuri:

- versiunea formatului de certificat;
- numărul serial;
- algoritmul de semnare;
- numele emitentului;
- perioada de valabilitate a certificatului, intervalul de timp în care certificatul poate fi operaţional;
- informaţiile de identificare a entităţii care deţine certificatul;
- cheia publică a proprietarului;
- identificatorul unic al emitentului;
- identificatorul unic al deţinătorului;
- semnătura digitală a Autorităţii de certificare etc.

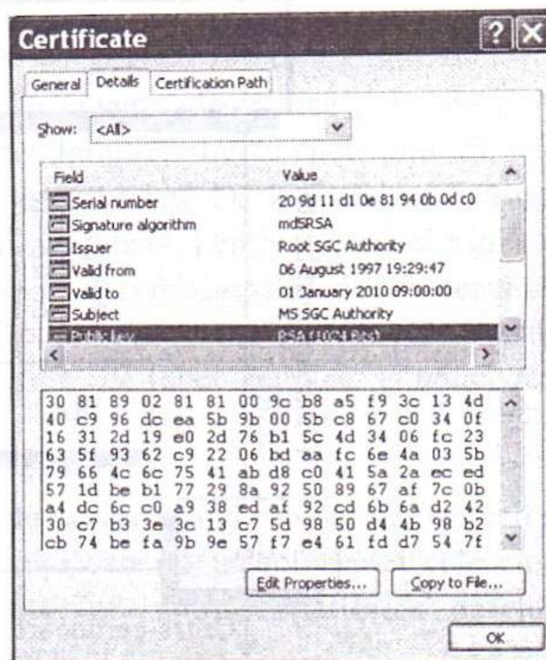


Figura 6.4.2. **Certificat digital**

Utilizarea certificatului digital garantează autenticitatea emitentului.

Autoritatea de certificare este autoritatea dintr-o reţea care generează şi administrează acreditările de securitate şi cheile publice pentru verificarea semnăturii mesajelor sau pentru criptare. Autoritatea de certificare îndeplineşte următoarele funcţii de bază:

- verifică informaţiile declarate de solicitantul de certificat digital (de cele mai multe ori, această sarcină este delegată Autorităţii de înregistrare);
- emite certificate – pentru entităţile finale şi pentru alte Autorităţi de certificare, astfel se atestă autenticitatea deţinătorului de cheie publică;
- gestionează informaţiile despre starea certificatelor şi generează lista de certificate revocate; certificatele pot fi revocate din diverse motive: este depăşită perioada de valabilitate, s-a pierdut dispozitivul care stochează certificatul, cheia privată a fost compromisă, unele dintre informaţiile stocate pe certificat nu mai sunt valide etc.
- semnează certificatele digitale şi listele de certificate revocate cu cheia sa privată;
- publică periodic lista de certificate revocate;
- arhivează certificatele expirate, pentru rezolvarea unor probleme care pot să apară ulterior.

Acţiunile Autorităţii de certificare sunt guvernate de un set de reguli denumite instrucţiuni practice de certificare (CPS – *Certification Practice Statement*).

Autoritatea de înregistrare are rolul să verifice solicitările utilizatorilor pentru emiterea de certificate digitale şi să comunice Autorităţii de certificare rezultatele valide. Autoritatea de înregistrare este o componentă opţională a infrastructurii de chei publice, având rolul de a elibera Autoritatea de certificare de unele dintre sarcinile sale, cum ar fi:

- verificarea informaţiilor declarate de solicitantul de certificat digital (autentificarea persoanei);
- verificarea drepturilor entităţilor să obţină anumite tipuri de certificate;
- verificarea că entitatea deţine cheia privată care a fost înregistrată şi care corespunde cheii publice cerute pentru certificat. Aceasta este cunoscută sub numele de "dovada deţinerii" (*proof of possession* - POP);
- raportarea cheilor compromise sau expirate, situaţii în care certificatele vor fi revocate;
- alocarea de parole de acces entităţilor, necesare pentru înregistrarea şi eliberarea certificatelor digitale de Autoritatea de certificare;
- generarea perechilor de chei (cheie privată – cheie publică) pentru entităţi;
- iniţierea procesului de înregistrare la Autoritatea de certificare;
- iniţierea procesului procesului de recuperare a cheilor;
- arhivarea cheilor private;
- distribuirea dispozitivelor criptografice (*token, smart card*) conţinând cheile private.

Depozitul de certificate este componenta PKI folosită pentru publicarea certificatelor valide şi a celor revocate. CRL-ul este un instrument pentru verificarea validităţii certificatelor pentru care Autoritatea de certificare este responsabilă.

6.5. Utilizarea criptografiei în protocoalele OSI

Soluţiile de securitate folosite în reţelele de calculatoare apelează în mod frecvent la algoritmi criptografici. Criptografia este aplicată la toate nivelurile modelului de referinţă OSI (respectiv modelului arhitectural TCP/IP), cu excepţia nivelului fizic. Protocoale şi sisteme de securitate utilizate în mod obişnuit pentru a furniza diferite niveluri de protecţie serviciilor dintr-o reţea de calculatoare sunt prezentate în figura 6.5.1

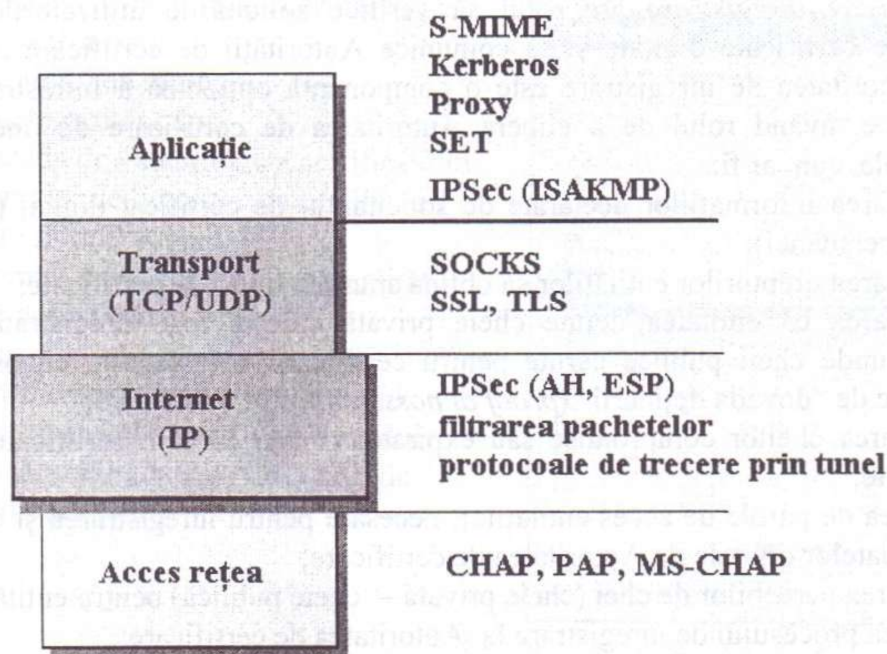


Figura 6.5.1. **Soluţii de securitatea în arhitectura TCP/IP**

PPTP (***Point-to-Point Tunneling Protocol***) funcţionează la nivelul 2 (legătura de date) al modelului de referinţă OSI şi are la bază standardul PPP pentru transmiterea serială a datelor prin linia telefonică. PPTP împachetează datele în cadre PPP şi apoi încapsulează pachetele PPP în datagrame IP pentru transmiterea lor printr-un tunel VPN (*Virtual Private Network*) prin internet. Astfel, PPTP permite extinderea reţelelor private ale întreprinderilor, prin utilizarea unor tuneluri proprii în infrastructura Internet, obţinându-se o reţea privată virtuală. Pachetele sunt încapsulate utilizându-se o formă de direcţionare generică (*GRE - Generic Routing Encapsulation*).

Criptarea datelor este o parte vitală a proceselor care au loc într-o reţea privată virtuală. PPTP utilizează mecanismele oferite de protocolul PPP pentru menţinerea conexiunii, încapsularea pachetelor şi pentru autentificarea utilizatorilor. Pentru autentificare, PPTP foloseşte cele două protocoale: ***CHAP*** (*Challenge Handshake Authentification Protocol*) şi ***PAP*** (*Password Authentification Protocol*).

CHAP este un protocol de autentificare utilizat pentru conectarea unui utilizator la un server de acces la internet oferit de un provider. Prin CHAP se verifică în mod periodic identitatea unui client, ori de câte ori server-ul va solicita această operaţie.

EAP (*Extensible Authentification Protocol*) - este un protocol de autentificare extinsă care acţionează la nivelul legăturii de date (la nivelul adresei MAC) în reţelele necablate. EAP oferă un mecanism prin care metoda de autentificare utilizată prin

protocolul PPP devine mai puternică. Prin EAP se adaugă protocolului PPP suport pentru o serie de scheme de autentificare, printre care carduri inteligente, Kerberos, chei publice, One Time Passwords. În prezent, majoritatea metodele de autentificare folosite de EAP sunt utilizate pentru înregistrarea clienților pe un server.

Rețelele private virtuale utilizează diverse mecanisme și protocoale pentru: transmisia prin tunele, obținerea confidențialității (prevenirea accesului neautorizat), autentificarea emițătorului (prevenirea alterării identității) și integritatea mesajelor (prevenirea alterării mesajelor). Atunci când metodele și tehnicile sunt bine alese, implementate și utilizate, pot furniza comunicații securizate peste o infrastructură publică.

Pentru asigurarea securității într-o rețea privată virtuală, în afara protocolului PPTP, se mai pot folosi următoarele protocoale:

- *L2F* (*Layer 2 Forwarding*) - dezvoltat de Cisco;
- *L2TP* (*Layer 2 Tunnelling Protocol*) - dezvoltat printr-o colaborare între Microsoft și Cisco;
- *IPSec* (*Internet Protocol Security*) constituie suport pentru tunelare, asigură securitate la nivelul rețea, din modelul de referință OSI/ISO, prin furnizarea unui canal securizat pentru datele transmise prin rețea. Gradul de securitate are la bază antetul de autentificare, criptarea sau ambele;

Protocolul L2TP este o combinație între modul de transmisie folosit de compania Cisco Systems Inc. la nivelul 2 și PPTP. Au fost preluate avantajele oferite prin cele două abordări. L2TP este mult mai flexibil decât PPTP, iar utilizarea lui necesită, față de implementarea PPTP, mai multe resurse din partea sistemului de calcul. L2TP operează ca un protocol al nivelului 2 din modelul de referință OSI.

IPSec reprezintă un set de specificații pentru servicii de autentificare, integrare și confidențialitate, bazate pe criptografie la nivelul datagramei IP. IPSec a devenit standardul *de facto* folosit pentru construirea unor tuneluri încapsulate și a rețelelor virtuale private pe internet. IETF (*Internet Engineering Task Force*) a acceptat IPSec, care este descris în RFC[1]-urile 2401, 2402 și 2406, printre altele. IPSec oferă entităților implicate în comunicație servicii standardizate.

---

[1] *Request for Comments* este un mecanism pentru dezvoltarea ansamblului de protocoale din internet. *Internet Architecture Board* (IAB) menține o listă cu RFC-urile publicate. Un document RFC, de obicei, se referă la un protocol din internet care poate fi în una din stările: standard, posibil standard, propunere de standard, experimental, informare, istoric. Fiecare protocol poate avea un anumit statut: se cere, este recomandat, utilizarea este limitată sau nu este recomandat.

IPSec poate fi utilizat în două moduri:

- *modul transport* – antetul IPSec este inserat după antetul IP. Câmpul *Protocol* din antetul IP este schimbat, pentru a specifica existenţa antetului IPSec după un antet IP normal. Antetul IPSec conţine informaţii pentru securizare: identificator SA, un nou număr de secvenţă şi posibilitatea de verificare a integrităţii datelor;
- *modul tunel* – întregul pachet IP, antetul şi celelalte câmpuri, sunt încapsulate într-un nou pachet, cu un antet IP complet nou. Modul tunel este utilizat, în general, când capătul terminal al unui tunel este altul decât destinatarul final. În unele cazuri, capătul terminal al unui tunel este un calculator cu rol de *gateway* de securitate.

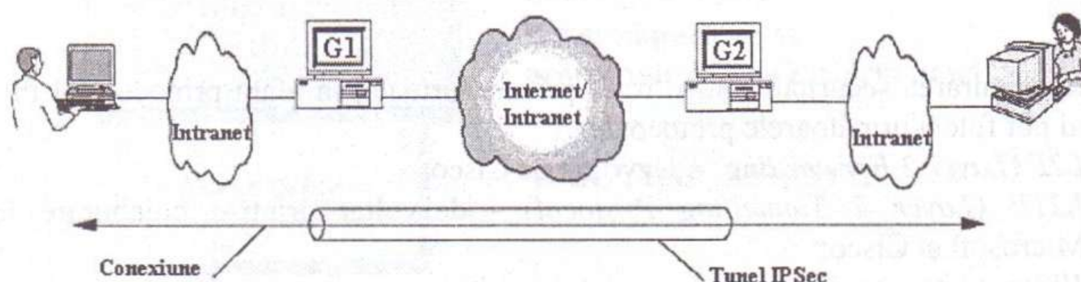


Figura 6.5.2. **Utilizarea IPSec ca suport pentru VPN**

- La nivelul transport se utilizează **protocolul SSL** (*Secure Socket Layer*) dezvoltat de Netscape Communications pentru a asigura securitatea transferului informaţional între aplicaţiile cu arhitectura client-server din internet. SSL oferă facilităţi de securitate prin autentificarea serverelor şi clienţilor şi prin criptarea comunicaţiei. Protocolul SSL este independent de protocoalele nivelului aplicaţie, care operează în mod normal peste TCP. Astfel, HTTP, FTP, SMTP şi Telnet pot funcţiona cu SSL;
- **TSL** *(Transport Layer Security)* este o dezvoltare a protocolului SSL versiunea 3.0. TLS permite clienţilor să autentifice serverele şi, facultativ, serverelor să autentifice clienţii. Canalul de transmisie este sigur, comunicaţiile fiind criptate. Între SSL 3.0 şi TLS 1.0 sunt mici diferenţe; dar este foarte probabil ca pe viitor TLS să cunoască o dezvoltare puternică;
- **PCT** *(Private Communications Technology),* standard dezvoltat de Microsoft, recunoaşte autentificarea şi criptarea pentru asigurarea confidenţialităţii comunicaţiilor prin internet.

Protocolul SSL este independent de platformă şi de aplicaţie, este bazat pe un standard deschis, fiind la ora actuală cel mai folosit protocol pentru securizarea conexiunilor în mediul internet. Standardul pentru SSL oferă servicii de autentificare, compresie de date, criptare şi integritatea datelor. Setul de protocoale numite SSL operează peste protocolul TCP, putând fi folosit pentru a asigura securitatea comunicaţiei protocoalelor de la nivelul aplicaţiei. Protocolul SSL este transparent

aplicației care îl folosește. Odată ce amândouă părțile implicate în comunicație sunt echipate cu implementări ale protocolului SSL, datele aplicației ar trebui să circule prin conexiunile securizate în același mod cum ar trece prin cele nesecurizate.

SSL oferă aplicațiilor de tipul client/server posibilitatea să comunice folosind o metodă ce nu permite ascultarea, interceptarea sau falsificarea informațiilor schimbate între cele două părți.

Principalul scop al protocolului SSL este acela de a realiza securitatea conexiunii între două entități, element esențial în realizarea unui sistem distribuit. Securitatea conexiunii se referă la asigurarea celor trei proprietăți de bază:

- *confidențialitatea* datelor prin conexiune – se realizează prin sistemul criptografic cu cheie simetrică (algoritmii DES, RC2, RC4, IDEA etc.);
- *autentificarea* entităților implicate în comunicație prin folosirea sistemelor criptografice cu cheie publică; de exemplu, RSA, DSS etc. Prin autentificarea părților implicate se elimină refuzul acestora de a recunoaște că au comunicat (*nerepudierea*);
- *integritatea* datelor transmise prin conexiune – transportul mesajelor include și o verificare a integrității acestora prin folosirea unui cod de autentificare a mesajului. Pentru calcularea codului de autentificare sunt folosite funcții de dispersie, cum ar fi SHA-1 sau MD5.

Dezavantajul protocolului SSL este acela că o conexiune SSL trebuie să folosească un socket TCP dedicat.

S/MIME (*Secure/Multipurpose Internet Mail Extensions*) a fost dezvoltat de RSA Data Security și se ocupă de transmiterea mesajelor de poștă electronică de tip MIME în internet, fiind semnate electronic și criptate cu cheie publică. Standardul S/MIME definește un nou tip de conținut MIME: application/x-pkcs7-mime. Standardul PKCS (*Public Key Cryptography Standard*), prin specificația PKCS#7, definește structurile de date și procedurile pentru semnătura digitală și criptarea altor structuri de date. Standardul S/MIME autentifică identitatea emițătorului și receptorului, verifică integritatea mesajului și garantează confidențialitatea conținutului mesajului, inclusiv al fișierelor atașate.

SSH (*Secure Shell*) este unul dintre cele mai populare protocoale utilizate pentru deschiderea unei sesiuni de comunicare pe un calculator de la distanță. SSH funcționează într-un mod asemănător cu telnet, dar are capacitatea de securizare a transmisiei. SSH va cripta în mod automat toate datele transmise în rețea, inclusiv parole, fișiere binare și comenzi de administrare, și tot în mod automat vor fi decriptate datele la recepție. Rezultatul este criptarea *transparentă*: utilizatorul lucrează normal, el nu este interesat de criptarea mesajelor transmise prin rețea.

SSH are o arhitectură client-server. Un program *server SSH* este instalat şi se execută pe un sistem cu rol de administrator, care acceptă sau respinge conexiunile la calculatorul-gazdă. Pentru lansarea unor comenzi, utilizatorii au instalate şi vor executa *programe client SSH*.

Protocolul SSH oferă autenticitatea, criptarea şi integritatea datelor transmise prin reţea. Produsele software care au la bază protocolul SSH sunt disponibile pe aproape orice platformă de calculatoare: Unix, Microsoft Windows, Macintosh etc. Produsele SSH permit accesul de la distanţă la resursele unui calculator şi execuţia unor operaţii de bază, cum ar fi: lansarea de comenzi, transferul de fişiere şi retransmisia printr-un port. Aceste produse SSH includ diverse metode de criptare (DES, 3DES, IDEA etc.) şi metode de autentificare (RSA, DSA – *Digital Signature Alghoritm*). Protocolul este implementat şi acţionează la **nivel aplicaţie**.

S/HTTP *(Secure HyperText Transfer Protocol)* este un protocol al nivelului aplicaţie folosit în comunicaţiile securizate dintre clienţii şi serverele Web. S/HTTP este compatibil cu HTTP, fiind un protocol de comunicaţie orientat pe mesaje care oferă servicii de securitate: confidenţialitatea tranzacţiilor, integritatea datelor, nerepudierea originii datelor. S/HTTP transmite mesaje sau pachete securizate, între clientul şi serverul web, prin stabilirea unei conexiuni de tip SSL.

SET (*Secure Electronic Transaction*) reprezintă un standard deschis pentru domeniul comercial, având capacitatea de a securiza tranzacţiile prin cărţi de credit pe internet. A fost dezvoltat de Visa, MasterCard, IBM, Microsoft. Protocolul are la bază certificatele digitale. SET defineşte rolurile şi relaţiile între părţile implicate în tranzacţiile pe internet, care sunt cerinţele de securitate şi cum pot fi îndeplinite.

6.6. Test de evaluare a cunoştinţelor

1. O semnătură digitală conţine un rezumat al mesajului ce se referă la:
   a. arată dacă mesajul a fost alterat după transmisie;
   b. defineşte algoritmul de criptare;
   c. confirmă identitatea celui ce a trimis mesajul;
   d. permite transmiterea mesajului într-un format digital.

2. Care dintre următoarele afirmaţii este cea mai bună tehnică pentru a asigura securitatea în timpul transmisiei datelor?
   a. jurnalul de comunicaţii;
   b. jurnalul software-ului de sistem;
   c. criptarea;
   d. protocolul standard.

3. Crearea unei semnături electronice:
   a. criptează mesajele;
   b. verifică de unde a venit mesajul;
   c. nu poate fi compromisă când se utilizează cheie privată;
   d. nu poate fi utilizată cu sisteme de e-mail.

4. Care dintre următoarele afirmații este cea mai evidentă metodă de autentificare a expeditorului?
   a. semnătura digitală;
   b. criptografia asimetrică;
   c. certificatul digital;
   d. codul de autentificare a mesajului.

5. Care dintre următoarele afirmații gestionează ciclul de viață al certificatelor digitale pentru a asigura că securitatea adecvată și controalele există în aplicațiile semnăturii digitale raportate la e-comerț?
   a. autoritatea de înregistrare;
   b. autoritatea de certificare (CA);
   c. lista revocării certificatelor;
   d. declarația de utilizare a certificatelor.

6. Semnătura digitală cere ca:
   a. expeditorul (cel care semnează) să aibă o cheie publică și destinatarul să aibă o cheie privată;
   b. expeditorul să aibă o cheie privată și destinatarul să aibă o cheie publică;
   c. expeditorul și destinatarul să aibă o cheie publică;
   d. expeditorul și destinatarul să aibă o cheie privată.

7. Viitoarea semnătură digitală care asigură expeditorul că nu poate nega mai târziu că a generat și a trimis mesaje asigură:
   a. integritatea datelor;
   b. autenticitatea;
   c. nonrepudierea;
   d. protecția retrimiterii.

8. Când utilizăm criptarea cu cheie publică pentru a securiza datele ce au fost transmite prin intermediul reţelei de calculatoare, trebuie să avem:
   a. cele două chei de criptare şi decriptare sunt chei publice;
   b. cheia folosită pentru criptare este privată, iar cheia folosită pentru decriptare este publică;
   c. cheia folosită pentru criptare este publică, iar cheia folosită pentru decriptare este privată;
   d. ambele chei de criptare şi decriptare sunt chei private.

9. O utilizare eficientă a PKI trebuie să cripteze:
   a. mesajul întreg;
   b. cheia privată;
   c. cheia publică;
   d. cheia simetrică.

10. Autenticitatea şi confidenţialitatea mesajului e-mail sunt atinse semnând mesajul utilizând:
   a. cheia privată a expeditorului şi criptarea mesajului utilizând cheia publică a destinatarului;
   b. cheia publică a expeditorului şi criptarea mesajului utilizând cheia privată a destinatarului;
   c. cheia privată a destinatarului şi criptarea mesajului utilizând cheia publică a expeditorului;
   d. cheia publică a destinatarului şi criptarea mesajului utilizând cheia privată a expeditorului.

Capitolul 7

Continuarea activităţii şi refacerea după dezastre

Capitolul 7

Continuarea activității și refacerea după dezastre

7.1. Continuarea activității. Planificarea refacerii după dezastre

Activitatea oricărei organizații este expusă unei multitudini de riscuri care pot produce afectări ale activității, pierderi materiale, financiare, umane sau pot afecta imaginea acesteia. În aceste condiții este esențial ca managementul să stabilească drept obiectiv strategic crearea unei culturi organizaționale menite să permită identificarea și managementul riscurilor care se pot produce. Astfel de riscuri sunt reprezentate de:

- imposibilitatea de a asigura servicii critice destinate clienților;
- afectări ale cotei de piață, imaginii, reputației sau brandului;
- eșecul în protejarea activelor, inclusiv activele de natura proprietății intelectuale sau personalul;
- eșecul controlului afacerii;
- imposibilitatea asigurării conformității în raport cu legislația și cadrul de reglementare.

Scopul procesului de continuare a activității/refacerii după dezastre (*business continuity/desaster recovery*) este să permită organizației să-și deruleze afacerea oferind serviciile critice în cazul producerii unor evenimente distructive și să poată face față unei întreruperi a sistemului său informațional. Pentru astfel de evenimente este necesar să se elaboreze planuri de reluare a activității și să se asigure resursele necesare.

Planificarea continuării activității (*Business Continuity Planing – BCP*)[1] reprezintă procesul proiectat pentru reducerea riscurilor activității organizației apărute ca urmare a întreruperii neașteptate a funcțiilor/operațiilor critice, manuale sau automate, necesare pentru supraviețuirea organizației. Sunt cuprinse resursele materiale și umane necesare în vederea asigurării unui nivel minim pentru operațiile critice.

Planul de continuare a activității este urmarea conștientizării impactului producerii unor evenimente de tipul dezastre naturale, defecțiuni tehnologice, erori umane sau terorism, a înțelegerii necesității de a fi pregătit pentru astfel de evenimente obiectivele urmărite fiind reprezentate de minimizarea pierderilor financiare, continuarea activității curente pentru asigurarea serviciilor solicitate de clienți,

---

[1] CISA.

limitarea distrugerilor, a afectării reputaţiei, lichidităţii, poziţiei în piaţă şi asigurarea conformităţii cu legile şi regulamentele în domeniu.

BCP este un proces complex desfăşurat în mai multe etape. Prima dintre acestea, şi extrem de importantă prin ieşirile pe care le oferă, este reprezentată de evaluarea riscurilor. Această etapă are rolul de a identifica cele mai importante procese care susţin activitatea organizaţiei. BCP se va construi plecându-se de la aceste procese critice asigurând continuarea operaţiilor în cazul producerii evenimentelor distructive.

BCP intră în sfera de responsabilitate a senior-managementului însărcinat cu asigurarea protecţiei activelor şi a viabilităţii organizaţiei. Senior-managementul este răspunzător de managementul riscurilor la nivelul organizaţiei şi de aceea aprobarea şi monitorizarea modului de implementare a BCP reprezintă una dintre responsabilităţile sale. Implicarea top-managementului în elaborarea planului este esenţială prin natura soluţiilor adoptate, prin resursele disponibilizate în acest sens şi nu în ultimul rând prin mutaţiile produse chiar în cultura organizaţională.

BCP trebuie să privească toate funcţiile şi activele organizaţiei. Fiecare entitate organizaţională trebuie să asigure un nivel minim de funcţionalitate imediat ce se produce întreruperea activităţii din cauza unui eveniment distructiv.

BCP include proceduri de refacere în urma dezastrelor (*disaster recovery procedures* – DRP) şi planul de continuitate al operaţiilor. Dacă DRP este planul destinat reluării activităţilor operaţionale la nivelul entităţilor organizaţionale, în cazul sistemelor informaţionale DRP cuprinde procedurile necesare refacerii proceselor IT. Planul de refacere pentru sistemele informaţionale trebuie perceput ca parte, dar şi suport al întregului plan de continuare a activităţii. BCP ia în considerare operaţiunile-cheie cele mai importante pentru supravieţuirea organizaţiei, precum şi resursele materiale şi umane care să le susţină.

BCP cuprinde:

- DRP (*Disaster Reocovery Plan*), necesar în refacerea facilităţilor devenite neoperabile, incluzând relocarea operaţiilor într-o nouă locaţie;
- planul operaţiunilor (*Operations Plan*), necesar entităţilor organizaţionale în efortul de refacere;
- planul de restaurare (*Restoration Plan*), necesar reluării operaţiilor într-o locaţie refăcută sau una nouă.

Partea de operaţiuni a BCP trebuie să privească toate funcţiile şi activele necesare. Soluţia unor facilităţi alternative este o ultimă decizie determinată de costurile implicate.

Aşa cum arătam, primul pas în realizarea BCP este reprezentat de analiza riscurilor. Pentru aceasta este necesară identificarea ameninţărilor asupra activelor. În cazul DRP activele sunt reprezentate de componentele sistemului informaţional. Riscul este direct proporţional cu valoarea activului şi probabilitatea apariţiei ameninţării. Clasificarea aplicaţiilor informatice depinde de natura businessului şi importanţa aplicaţiei pentru business. În egală măsură, valoarea este dată şi de importanţa aplicaţiei în raport cu strategia organizaţiei. Componentele sistemului informaţional sunt adecvate aplicaţiilor (valoarea calculatoarelor şi a reţelei sunt determinate de importanţa aplicaţiei care le foloseşte).

Scopul BCP este de a identifica ce trebuie să se întâmple la nivelul afacerii atunci când se produce un dezastru. De aceea o componentă a BCP este planul IT de refacere în urma unui dezastru (*IT Disaster Recovery Plan*). Acesta detaliază procedurile ce urmează a fi executate de specialiştii IT în scopul refacerii sistemului informaţional. DRP poate fi inclus în BCP sau poate constitui un document distinct în funcţie de nevoile organizaţiei.

Este necesar să subliniem faptul că nu toate sistemele trebuie să prezinte o strategie de refacere. În baza rezultatelor analizei riscurilor, managementul poate considera că din punct de vedere al eficienţei economice (raportul cost-beneficiu) anumite aplicaţii nu trebuie refăcute în cazul producerii unui dezastru.

Concluzionând, conceptul de planificare a continuităţii activităţii înseamnă o combinaţie între planificarea refacerii în caz de dezastre şi continuitatea operaţiunilor activităţii. În funcţie de complexitatea activităţii, pot fi elaborate unul sau mai multe planuri acoperind diferitele aspecte ale continuării activităţii şi refacerii, dar fiecare dintre acestea trebuie să fie coroborat cu celelalte planuri pentru a se asigura o strategie BCP viabilă.

7.2. Continuitatea sistemelor informaţionale. Planificarea refacerii în urma dezastrelor

Continuitatea sistemelor informaţionale. Planificarea refacerii în urma dezastrelor (*IS Business Continuity/Disaster Recovery Planning*) reprezintă o componentă importantă a BCP şi strategiei de refacere în caz de dezastru. Procesarea prin mijloace IT este de importanţă strategică deoarece aproape toate procesele afacerii utilizează resursele IT. În aceste condiţii devine necesară existenţa unei facilităţi pentru procesarea informatică pregătită a fi operaţională în momentul producerii unui dezastru. Dacă este realizat ca plan de sine stătător, planul SI trebuie să fie în conformitate cu BCP.

7.2.1. Dezastre și alte evenimente distructive

Dezastrele determină inoperativitatea resurselor informaționale afectate pentru o perioadă de timp fiind astfel afectată desfășurarea normală a activității. Întreruperea poate să dureze de la câteva ore la câteva zile, în funcție de amploarea distrugerilor care au afectat resursele informaționale. Acest fapt determină eforturi de refacere a statusului operațional.

Un dezastru poate fi produs de calamități naturale cum ar fi cutremure, inundații, tornade, furtuni puternice, incendii etc. care produc distrugeri extinse facilității de procesare și localității în care aceasta se află. Alte dezastre pot să apară când servicii vitale cum ar fi furnizarea de energie electrică și/sau gaz, telecomunicațiile sau alte servicii nu mai pot fi asigurate de furnizori. Tot în categoria dezastrelor includem atacurile teroriste, atacurile hackerilor, virușii și erorile umane.

Este bine să precizăm faptul că nu toate întreruperile în asigurarea serviciilor critice pot fi considerate ca dezastre. Este cazul funcționării defectuoase a sistemelor, deteriorarea accidentală a fișierelor, „căderea" rețelei etc. Acestea reprezintă evenimente cu risc înalt, dar chiar dacă necesită refacerea componentelor hardware, a fișierelor sau a software-ului nu se vor regăsi în BCP. Un bun BCP va lua în considerare toate tipurile de evenimente având impact critic asupra facilităților de procesare automată și activitatea curentă a utilizatorilor finali. În cazul scenariilor celor mai grave vor trebui stabilite strategii pe termen scurt și lung. În cazul strategiilor pe termen scurt se poate opta pentru facilități de procesare alternativă pentru acoperirea nevoilor operaționale imediate. Pe termen lung, se impune o nouă facilitate permanentă echipată astfel încât să asigure continuitatea proceselor normale ale SI.

Zvonurile referitoare la producerea unor incidente serioase pot avea sau nu surse interne, pot avea sau nu corespondent în realitate, dar consecințele lor pot fi devastatoare, putând să determine chiar pierderea încrederii clienților și a partenerilor de afaceri în organizație și scăderea valorii de piață a acesteia. De aceea activitățile de PR (*public relations)* pot să joace un rol important în protejarea imaginii organizației și asigurarea faptului că nu se va ajunge la acutizarea crizei. Pentru aceasta este necesară respectarea cerințelor de bună practică în cazul incidentelor majore. Declarațiile publice vor trebui să prevină/restrângă impactul negativ asupra opiniei publice și impactul financiar al zvonurilor.

7.2.2. Procesul BCP

Procesul BCP se desfăşoară în următoarele faze ale ciclului de viaţă:

1. crearea unei politici privind continuitatea activităţii şi refacerea după dezastru;
2. analiza impactului asupra activităţii (*Business Impact Analysis* – BIA);
3. clasificarea operaţiilor şi analiza critică;
4. elaborarea BCP şi a procedurilor de refacere (DRP);
5. instruirea cu privire la BCP şi conştientizarea importanţei lui;
6. testarea şi implementarea planului;
7. monitorizarea.

Politica de continuitate a activităţii şi de refacere în caz de dezastru trebuie să fie pro-activă şi să înglobeze controale preventive, detective şi corective. BCP este cel mai critic control corectiv şi este dependent de alte controale, în particular managementul incidentelor şi backup-ul. De aceea este necesar ca grupul pentru managementul incidentelor să prezinte o componenţă adecvată, pregătită în managementul de criză, iar BCP să fie corect proiectat, documentat, testat, fundamentat şi auditat.

Managementul incidentelor BCP

Literatura de specialitate evidenţiază necesitatea ca managementul să înţeleagă caracteristicile asociate unei crize. Aceste caracteristici sunt reprezentate de:

- elementul-surpriză;
- lipsa unor informaţii;
- pierderea (în mai mare sau mai mică măsură) a controlului;
- escaladarea cursului evenimentelor;
- panică etc.

Spre deosebire de criză, un incident este un eveniment neaşteptat, care nu cauzează pagube importante. Incidentele şi crizele au o natură dinamică. Ele evoluează în timp şi, datorită circumstanţelor nou-apărute, sunt adesea rapide şi neprevăzute. De aceea managementul lor trebuie să fie dinamic, proactiv şi bine documentat. În funcţie de rezultatul estimării nivelului consecinţelor distrugerii asupra activităţii, toate incidentele trebuie clasificate. Clasificarea incidentelor poate include următoarele categorii:

- **neglijabil** – incident care nu produce distrugeri semnificative sau distrugerile sunt neperceptibile („căderi" ale sistemului de operare urmate de recuperarea completă a informaţiilor, „căderi" ale sursei de energie suplinite de UPS-uri);
- **minor** – sunt evenimente care deşi nu sunt neglijabile nu produc un impact material sau financiar negativ;

- **major** – incidente care produc impact material negativ asupra proceselor afacerii şi pot afecta alte sisteme, departamente sau chiar parteneri de afaceri (clienţii);
- **criză** – este un incident major care poate avea un impact material serios asupra continuităţii afacerii şi poate afecta negativ alte sisteme şi terţi. Severitatea incidentului este direct proporţională cu intervalul scurs între începutul incidentului şi momentul refacerii în urma impactului produs.

Incidentele minore, majore şi crizele trebuie documentate, clasificate şi urmărită soluţionarea lor. Acesta este un proces dinamic, deoarece un incident major poate să descrească în intensitate pentru ca mai târziu să se extindă şi să producă o criză. Incidentele neglijabile pot fi analizate statistic cu scopul identificării unor cauze sistemice sau evitabile.

Ofiţerul de securitate sau orice altă persoană desemnată trebuie să notifice toate incidentele de îndată ce un eveniment se produce urmând un protocol prestabilit. În conformitate cu această procedură va fi contactat purtătorul de cuvânt, va fi informat managementul sau vor fi anunţate organizaţiile de reglementare implicate.

Analiza impactului asupra activităţii (Business Impact Analysis)

BIA reprezintă un pas important în elaborarea BCP. Această etapă are ca scop identificarea evenimentelor care pot să apară afectând continuitatea operaţională a organizaţiei, generând un impact negativ asupra situaţiei financiare, resurselor umane şi reputaţiei organizaţiei.

Desfăşurarea acestei faze presupune o bună cunoaştere a organizaţiei, a proceselor-cheie şi a resurselor IT necesare susţinerii acestor procese. De aceea este necesară identificarea aplicaţiilor şi datelor critice, reţelelor, sistemelor software, facilităţilor, proces realizat cu aprobarea managementului.

În desfăşurarea BIA se pot utiliza mai multe abordări:

- **utilizarea de chestionare** – presupune utilizarea de chestionare detaliate destinate utilizatorilor IT cheie şi utilizatorilor finali;
- **derularea de interviuri** la nivelul grupurilor de utilizatori cheie;
- **discuţii cu utilizatorii finali şi responsabilii IT,** cu scopul estimării impactului posibil ca urmare a producerii unor întreruperi de amploare diferită.

Realizarea BIA presupune soluţionarea a trei probleme majore:

1. identificarea proceselor critice pentru organizaţie;
2. identificarea resurselor informaţionale critice specifice proceselor critice identificate în primul pas;

3. determinarea timpului critic de refacere a resurselor informaţionale în care procesele afacerii trebuie reluate înainte de a se înregistra pierderi semnificative sau inacceptabile. Spre exemplu, instituţiile financiare sau de brokeraj vor determina timpi critici de refacere mult sub cei determinaţi de întreprinderile cu profil de producţie, acest lucru fiind determinat de natura serviciilor prestate.

La nivelul unei organizaţii spre exemplu, este important ca pentru funcţiile critice să se determine durata maximă admisă a întreruperilor, informaţia urmând a fi sintetizată sub forma matricei funcţiilor critice (tabelul 7.2.1).

Tabelul 7.2.1

	Timp de întrerupere admis şi nivel minim de activitate necesitat				
Activităţi	< o zi	< 3 zile	<7 zile	< 14 zile	< 30 zile
A1	x				
A2		x			
A3	x				
A4			x		
A5				x	
A6					x

Pentru luarea acestei decizii sunt luaţi în considerare doi factori: **costul întreruperii** (*downtime cost*) provocat de dezastru şi respectiv **costul strategiei corective alternative** (figura 7.2.1).

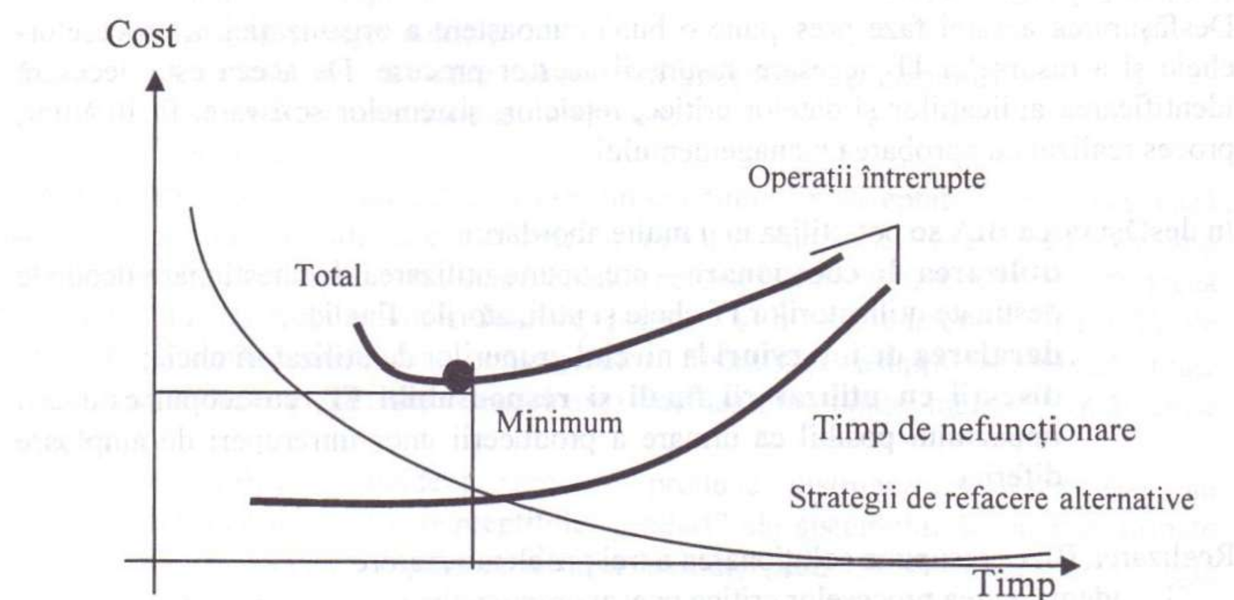


Figura 7.2.1 **Costul întreruperii vs. costul refacerii**

Costul întreruperii provocate de dezastru trebuie limitat deoarece înregistrează creșteri rapide în timp. În momentul în care el își încetează creșterea s-a atins punctul în care activitatea (afacerea) nu mai poate continua.

Costul strategiilor corective alternative scad odată cu obiectivele stabilite pentru timpul de refacere. Costul refacerii este format din costul:

- pregătirii și testării periodice a BCP;
- costul locațiilor destinate site-urilor de back-up;
- costul polițelor de asigurare;
- costul anual al locațiilor alternative.

Figura 7.2.1 evidențiază costul strategiilor alternative, costul întreruperilor, dar și costul total al întreruperii și refacerii. Scopul urmărit este reprezentat de identificarea punctului în care costul total este minim. Atingerea acestui punct se va realiza prin gândirea de soluții alternative. Curba din figura 7.2.1 numită strategiile de refacere alternative, este reprezentarea în fapt a mulțimii strategiilor posibile, fiecare strategie posibilă având un cost fix. Cu cât timpul de refacere cerut va fi mai scurt, cu atât costul fix va fi mai mare. Dacă strategia de continuare a activității presupune un timp de refacere mai mare, va fi mai puțin costisitoare, dar mai susceptibilă la costuri ale întreruperii evoluând în spirală, fără a mai putea fi controlate.

După identificarea activităților critice și aplicațiilor care le susțin, se procedează la identificarea amenințărilor în condițiile funcționării normale a sistemului. Specialiștii în domeniu recomandă identificarea tipurilor de amenințări care conduc la întreruperi ale funcționării sistemului, rezultatul acestei analize urmând să se materializeze într-o grilă în care prima coloană va indica tipul de amenințare, iar în coloana a doua se va preciza în ce măsură acesta a determinat incidente conducând la întreruperea funcționării sistemului (tabelul 7.2.2).

Tabelul 7.2.2

Tipul amenințării	**Procent**
Întreruperea alimentării cu energie electrică	35%
Factor uman (erori, sabotaj)	12%
Inundații	10%
Defecțiuni hardware	15%
Furtuni	8%
Incendii	10%
Cutremure	6%
Altele	4%

Probabilitatea producerii unor dezastre urmează a se determina în conjuncție cu analiza riscurilor și ținând seama de următorii factori:

- locaţia geografică;
- topografia locului;
- apropierea de sursele de energie electrică, ape, aeroporturi;
- apropierea de centrale nucleare;
- istoricul relaţiei cu furnizorii de utilităţi şi măsura în care aceştia au asigurat continuitate în furnizarea serviciilor.

Probabilităţile determinate vor lua una dintre următoarele valori: mare (10), mediu (5), mic (1). Probabilităţile vor fi apoi ponderate cu impactul estimat asupra funcţiilor de business sau facilităţilor:

- niciun impact sau întrerupere în operaţiuni (0);
- impact notabil, întreruperi de până la opt ore (1);
- afectarea echipamentului şi/sau facilităţilor, întreruperi în operaţii pentru opt până la 48 de ore;
- distrugeri majore ale echipamentului şi/sau facilităţilor, întreruperi ale operaţiilor pentru mai mult de 48 de ore.

Clasificarea operaţiilor şi analiza critică

Clasificarea riscurilor sistemului presupune determinarea riscurilor plecând de la impactul dat de timpul de refacere, precum şi de probabilitatea apariţiei întreruperilor. În acest scop se apreciază riscul apariţiei şi se determină costul probabil. Dacă riscul producerii incidentului distructiv în următorii cinci ani este de 1 la 1000 (0,1%), iar impactul este estimat la 10 milioane RON, costul maxim va fi de 10.000 RON anual. Prin acest proces de evaluare bazat pe riscuri se realizează prioritizarea sistemelor în efortul de dezvoltare a strategiilor de refacere. Participă la acest proces de evaluare personalul IT şi utilizatorii finali.

Prioritizarea iniţială a activităţilor în funcţie de importanţa acestora în realizarea obiectivelor strategice ale organizaţiei, realizată în faza de analiză a impactului asupra organizaţiei, poate fi modificată pe măsură ce procesele afacerii sunt modelate în cadrul scenariilor de simulare a diferitelor ameninţări. Pentru fiecare activitate critică şi sistem care o deserveşte se va proceda la identificarea ameninţărilor şi estimarea probabilităţii producerii lor.

Sistemele evaluate vor putea fi plasate în una dintre următoarele categorii:

- **critice** – aceste funcţii nu pot fi executate decât dacă sunt înlocuite cu capabilităţi identice. Nu vor putea fi înlocuite de metode manuale, toleranţa la întrerupere este foarte scăzută şi în consecinţă costul întreruperii este foarte ridicat;
- **vitale** – aceste funcţii pot fi realizate manual, dar pentru o scurtă perioadă de timp. Înregistrează toleranţă mai mare la întrerupere decât sistemele critice şi de aceea într-o oarecare măsură costul întreruperii este mai mic. Timpul de refacere este limitat la cinci zile sau mai puţin;

- **sensibile** – sunt funcții ce pot fi realizate manual, la un cost tolerabil pe o perioadă mai mare de timp;
- **nesensibile** – funcții ce pot fi întrerupte pe o perioadă mare de timp, la un cost scăzut (poate chiar să nu implice costuri) și necesită puțin (sau chiar deloc) timp pentru refacere.

Pasul următor în managementul continuității este reprezentat de identificarea diferitelor strategii de refacere și alternativele disponibile pentru refacere în urma unei întreruperi sau dezastru. În alegerea strategiilor de refacere vor fi avuți în vedere doi indicatori: obiectivul punctului de refacere (*recovery point objective* – RPO) și obiectivul timpului de refacere (*recovery time objective*- RTO). RPO este determinat în funcție de datele pierdute ca urmare a întreruperii operațiilor. RPO indică cel mai apropiat punct în timp în care se pot recupera datele. De aceea procedeele de back-up vor fi stabilite în raport de RPO.

Alternative de refacere

Orice platformă IT pe care se execută o aplicație susținând o funcție critică a afacerii are nevoie de o strategie de refacere. Alternativa adecvată din punct de vedere al costului de refacere și a costului impactului va trebui aleasă în funcție de nivelul relativ de risc stabilit prin BIA. Aceste strategii de risc includ:

- hot site-uri;
- warm site-uri;
- cold site-uri;
- facilități de procesare duplicată a datelor;
- site-uri mobile;
- convenții de reciprocitate stabilite cu alte organizații.

Hot site este reprezentată de site-uri configurate complet care pot fi operaționale în câteva ore. Echipamentul, rețeaua și sistemele software sunt compatibile cu site-ul operațional, fiind un backup al acestuia. Vor trebui asigurate următoarele resurse: personal specializat, programe, fișiere de date și documentații. Costul realizării unor asemenea site-uri este ridicat, de aceea se poate opta pentru un site oferit de o firmă specializată, în acest al doilea caz costul fiind mai scăzut. Indiferent de soluția aleasă, aceste costuri sunt justificate pentru aplicații critice, iar polița de asigurare va acoperi costurile utilizării unei astfel de facilități. Costul cuprinde: costul de înscriere, cheltuieli lunare, cheltuieli de testare, costuri de activare și costurile aferente orelor/zilelor de utilizare. Aceste site-uri sunt destinate operațiunilor urgente pentru o perioadă limitată de timp (în limita a câteva săptămâni). Utilizarea pe termen lung ar putea impieta protecția altor organizații înregistrate. Pentru disponibilizarea site-urilor hot, firme specializate pun la dispoziție site-uri warm sau cold pe care să se poată face migrarea după finalizarea refacerii operațiilor.

Warm site reprezintă site-uri parţial configurate, de obicei cu conexiuni la reţea şi echipament periferic, dar fără să dispună de un calculator principal, acest fapt fiind datorat costului ridicat al acestuia şi posibilităţii de a fi achiziţionat rapid la nevoie. De multe ori sunt dotate cu sisteme prezentând putere de calcul inferioară celei sistemului operaţional. Aducerea şi instalarea CPU, precum şi a celorlalte echipamente necesare poate dura câteva zile sau săptămâni, dar, după dotarea site-ului cu toate componentele necesare, acesta va deveni operaţional în câteva ore.

Cold site presupune existenţa doar a mediului de bază (reprezentat prin instalaţie electrică şi de aer condiţionat etc.) pentru procesarea informaţiei. Site-ul este pregătit pentru instalarea echipamentelor, niciun fel de echipament nefiind instalat dinainte. Un astfel de site poate deveni operaţional în câteva săptămâni.

Facilităţi de procesare duplicată a datelor reprezintă soluţii dedicate, fiind site-uri de refacere realizate de organizaţie care pot duplica aplicaţiile critice. Pot lua *forma site-urilor standby hot* prin acordul reciproc cu o altă companie de instalare. O astfel de soluţie conduce la mai puţine probleme de coordonare privind compatibilitatea şi disponibilitatea. Pentru ca o astfel de soluţie să fie viabilă vor trebui respectate unele principii, şi anume:

- site-ul ales nu trebuie să poată fi supus unui aceluiaşi dezastru care afectează site-ul supus duplicării;
- trebuie să existe o coordonare a strategiilor hardware şi software pentru a se putea asigura un grad rezonabil de compatibilitate în vederea realizării back-up-ului;
- trebuie asigurată disponibilitatea resurselor;
- trebuie să existe o înţelegere privind prioritatea adăugării de aplicaţii până când toate resursele pentru refacere sunt utilizate;
- este necesară testarea periodică, indiferent dacă site-urile duplicate sunt sub proprietate comună sau sunt sub acelaşi management.

Site-uri mobile, o soluţie recentă, constau în utilizarea unui trailer care poate fi rapid transportat la locaţia organizaţiei sau într-un site alternativ pentru a asigura facilitatea de procesare a informaţiei. Site-urile mobile pot fi conectate pentru a forma o arie de lucru lărgită şi pot fi pre-configurate cu servere, calculatoare desktop, echipament de comunicaţie, microwave şi sateliţi pentru legături de date. Astfel de soluţii sunt recomandate când în aria geografică a organizaţiei nu există facilităţi de refacere sau când dezastrul afectează arii extinse. Este o soluţie pentru duplicarea facilităţilor de procesare în cazul organizaţiilor caracterizate prin dispersia teritorială a unităţilor lor.

Convenţiile de reciprocitate stabilite cu alte organizaţii este o metodă mai puţin folosită. Se aplică atunci când în două sau mai multe organizaţii există echipament şi aplicaţii asemănătoare. Partenerii urmează să-şi pună reciproc la dispoziţie resursele

necesare în cazuri de urgență. Astfel de alternative prezintă avantajul unor costuri reduse și pot constitui unica alternativă disponibilă când site-urile hot, oferite de un unic furnizor, nu sunt disponibile. Dezavantajele sunt reprezentate de faptul că nu pot fi întotdeauna aplicabile, configurarea diferită a echipamentelor impune modificări în programe. În cazul realizării de modificări în configurarea echipamentelor, organizațiile nenotificate în acest sens vor beneficia în mod limitat de înțelegerea încheiată sau nu vor mai putea beneficia de aceasta.

Opțiunea pentru această alternativă presupune cunoașterea răspunsului la următoarele întrebări:

- Cât timp disponibil avem pe calculatorul site-ului-gazdă?
- Ce facilități, echipament și software vor fi disponibile?
- Va fi asigurat personal pentru asistență?
- Cât de repede poate fi obținut accesul la facilități?
- Legăturile pentru comunicațiile de date și voce pot fi stabilite pe site-ul-gazdă?
- Cât timp poate continua operarea de urgență?
- Cât de frecvent poate fi testat sistemul pentru compatibilitate?
- Cum va fi asigurată confidențialitatea datelor?
- Ce tip de securitate va fi permisă pentru sisteme și date?
- Există perioade de timp când facilitățile organizației partenere nu sunt disponibile?

Tehnologii de refacere

În cazul optării pentru soluția site-urilor oferite de terți, contractele ce urmează a se încheia trebuie să prezinte prevederi care să clarifice următoarele aspecte[2]:

1. *configurații*: configurațiile hardware și software oferite sunt adecvate nevoilor? Pot cunoaște modificări în timp?
2. *dezastre*: definirea dezastrului este suficient de extinsă pentru a acoperi nevoile anticipate?
3. *disponibilitatea*: în cât timp după producerea dezastrului facilitățile pot fi puse la dispoziție?
4. *numărul abonaților la site*: se limitează prin convenție numărul abonaților la site?
5. *numărul abonaților pe zonă*: se limitează prin convenție numărul abonaților în clădire sau zonă?
6. *preferințe*: cine are prioritate în cazul unor dezastre regionale? Utilizarea facilităților este exclusivă sau se va partaja spațiul cu alte organizații afectate de dezastru?

[2] Conform CISA.

7. *asigurare*: există o acoperire adecvată a asigurării pentru angajaţii companiei la site-ul de back-up? Asigurarea existentă va acoperi aceste cheltuieli?
8. *perioada de folosire*: cât timp este facilitatea disponibilă? Această perioadă este suficientă? Ce suport tehnic va oferi site-ul? Este adecvat?
9. *comunicaţii*: sunt comunicaţiile adecvate? Sunt conexiunile de comunicaţii de la site-ul de back-up suficiente pentru a permite comunicaţie nelimitată cu site-urile alternative la nevoie?
10. *garanţii*: ce garanţii va da furnizorul cu privire la disponibilitatea site-ului şi adecvarea facilităţilor?
11. *audit*: există o clauză care să permită auditul site-ului pentru o evaluare a securităţii logice, fizice şi a mediului?
12. *testare*: ce drepturi de testare sunt permise prin contract? Verificare împreună cu firma de asigurare a diminuărilor de despăgubiri ce pot interveni ca urmare a disponibilităţii site-ului.
13. *credibilitatea*: poate furnizorul dovedi credibilitatea oferită de site? Ideal, furnizorul trebuie să dispună de UPS, număr limitat de abonaţi, management tehnic solid, garanţii pentru compatibilitatea componentelor hardware şi software.

7.3. *Business Continuty* şi *Disaster Recovery*

Acest grup de funcţii trebuie să asigure coordonarea următoarelor activităţi:
- stabilirea datelor critice şi vitale ce urmează a fi stocate offsite;
- instalarea şi testarea sistemelor software şi aplicaţiilor în site-ul de recovery indiferent de natura acestuia – hot site, cold site etc;
- operarea din site-ul de recovery;
- rerutarea traficului în reţeaua de comunicaţii;
- restabilirea reţelei;
- transportul utilizatorilor în locaţia facilităţii de refacere;
- reconstruirea bazei de date;
- aprovizionarea cu consumabile;
- asigurarea şi achitarea cheltuielilor cu relocarea angajaţilor în locaţia de recovery;
- coordonarea utilizării sistemelor şi planificarea muncii angajaţilor.

Desfăşurarea acestor activităţi impune stabilirea unor echipe de lucru specializate, cu atribuţii bine stabilite, şi anume[3]:
- **echipa de stocare offsite** (*offsite storage team*) – echipă responsabilă cu obţinerea, pregătirea şi transportul datelor în locaţia centrului de recovery. Tot această echipă este responsabilă şi cu stabilirea şi urmărirea programului de stocare offsite a informaţiilor create prin operarea în centrul de recovery;

[3] Conform specificaţiilor CISA.

- **echipa software** (*software team*) – echipă responsabilă cu refacerea pachetelor software, încărcarea și testarea sistemelor de operare, rezolvarea problemelor la nivelul sofware-ului de bază;
- **echipa soft de aplicații** (*applications team*) – responsabilă cu refacerea aplicațiilor pe sistemele de back-up cerute în site-ul de recovery. Pe măsura avansării procesului de recovery, echipa are responsabilitatea monitorizării performanței aplicațiilor și integrității bazei de date;
- **echipa de securitate** (*security team*) are rolul de a monitoriza permanent securitatea sistemului și a legăturilor de comunicații, soluționarea incidentelor de securitate care afectează refacerea sistemului, asigură instalarea corespunzătoare și funcționarea software-ului de securitate. Răspunde totodată de securitatea activelor în perioada următoare producerii dezastrului;
- **echipa de operare de urgență** (*emergency operations team*) este formată din operatori de shift-are și supervizorii acestora care vor lucra în site-ul de recovery și vor conduce operarea de-a lungul întregii perioade a proiectelor de refacere. În sarcina acestei echipe poate fi și coordonarea instalării hardware-ului, dacă nu a fost stabilit drept centru de refacere un hot site sau o facilitate gata echipată;
- **echipa de refacere rețea** (*network recovery team*) este responsabilă cu rerutarea pe arii extinse a comunicațiilor de voce și date, restabilirea controlului rețelei gazdă și accesul la sistemul din centrul de recovery oferind susținerea pentru realizarea comunicațiilor de date și monitorizând integritatea comunicațiilor;
- **echipa de comunicații** (*communications team*) va colabora cu furnizorii de gateway în reroutarea serviciului local și a accesului gateway;
- **echipa de transport** (*transportation team*) asigură transportul angajaților la centrul de recovery, contactează angajații pentru a le comunica noile locații de lucru, planifică și aranjează cazarea angajaților;
- **echipa de echipamente utilizator** (*user hardware team*) stabilește locația și coordonează livrarea și instalarea echipamentelor utilizatorilor (terminale, imprimante, copiatoare etc.); oferă sprijin echipei de comunicații și participă la efortul de salvare a echipamentelor și facilităților.
- **echipa de pregătire date și înregistrări** (*data preparation and records team*) asigură actualizarea bazelor de date utilizate de aplicațiile din site-ul de recovery. Supraveghează personalul de introducere date și asistă activitatea de salvare a înregistrărilor în obținerea documentelor primare și a altor surse de introducere a datelor;
- **echipa de suport administrativ** (*administrative support team*) asigură suportul funcționarilor pentru celelalte echipe și asigură centrul de mesaje din site-ul de recovery. Poate asigura funcțiile de contabilitate și salarii și facilitățile necesare managementului;

- **echipa de aprovizionare** (*supplies team*) ajută echipa de echipamente utilizator să contacteze furnizorii şi coordonează logistica necesară aprovizionării cu cele necesare;
- **echipa de recuperare** (*savage team*) conduce relocarea proiectelor, realizează o evaluare mai detaliată, faţă de cea iniţială, a pagubelor înregistrate de facilităţi şi echipament, furnizează echipei de management de criză a informaţiilor necesare planificării privind reconstrucţia sau relocarea, oferă informaţiile privind completarea cererilor de despăgubiri şi coordonează efortul de salvare a înregistrărilor (refacerea documentelor şi a înregistrărilor pe medii de stocare electronică);
- **echipa de relocare** (*relocation team*) asigură coordonarea procesului de mutare din site-ul hot în noua locaţie sau în locaţia iniţială după refacerea acesteia. Aceasta presupune relocarea sistemelor de procesare a operaţiilor, a traficului de comunicaţii şi operaţii utilizator. Monitorizează tranziţia către un nivel normal al serviciilor;
- **echipa de coordonare** (*coordination team*) răspunde de coordonarea efortului de refacere în diferitele locaţii;
- **echipa juridică** (*leagal affairs team*) asigură soluţionarea problemelor cauzate de incidentele produse sau de nondisponibilitatea serviciilor;
- **echipa de test pentru refacere** (*recovery test team*) răspunde de testarea diferitelor planuri şi analizarea rezultatelor testelor;
- **echipa de instruire** (*training team*) asigură instruirea cu privire la planul de continuare a activităţii şi a planului de refacere;

7.4. Componentele BCP

În funcţie de cerinţele şi dimensiunea organizaţiei, BCP poate fi format din unul sau mai multe planuri:

- planul de refacere (*Business Recovery Plan* - BRP);
- planul de continuitate a operaţiilor (*Continuity of Operations Plan* – COOP);
- planul pentru continuitatea suportului/ Planul evenimentelor IT neprevăzute (*Continuity of support plan/IT Contingency plan*);
- planul pentru comunicaţii în condiţii de criză (*Crisis Communication Plan*);
- planul de răspuns la incidente (*Incident Response Plan*);
- planul de refacere după dezastre (*Disaster Recovery Plan* -DRP);
- planul de protecţie persoane şi bunuri (*Occupant Emergency Plan* – OEPP).

Planul de reluare a afacerii oferă proceduri pentru refacerea operaţiunilor afacerii imediat după producerea dezastrului. Fără să se focalizeze pe componenta IT, aceasta este vizată doar ca suport al activităţii firmei.

Planul continuității operațiilor oferă procedurile și capabilitățile necesare susținerii funcțiilor strategice ale firmei printr-un site alternativ pentru mai mult de 30 de zile. Privește submulțimea misiunilor critice pentru firmă. Nu se centrează pe IT.

Planul evenimentelor IT neprevăzute (*IT Contingency Plan/ Continuity of Support Plan*) oferă proceduri și capabilități pentru refacerea unei aplicații importante sau a sistemului informatic. Vizează distrugerile sistemului informatic, procesele afacerii nefiind vizate.

Planul comunicațiilor în condiții de criză (*Crisis Communications Plan*) oferă proceduri pentru diseminarea informațiilor către angajații firmei și beneficiarii externi de informație.

Planul de răspuns la *cyber incidents* (*Cyber Incidents Response Plan*) oferă strategii pentru detectarea și răspunsul la incidente și limitarea efectelor produse de acestea.

Planul de refacere în caz de dezastre (*Disaster Recovery Plan*) oferă proceduri detaliate pentru a facilita refacerea capabilităților într-un site alternativ.

Planul de protecție persoane și bunuri (*Occupant Emergency Plan*) asigură proceduri coordonate pentru limitarea victimelor și a distrugerilor ca urmare a amenințărilor fizice.

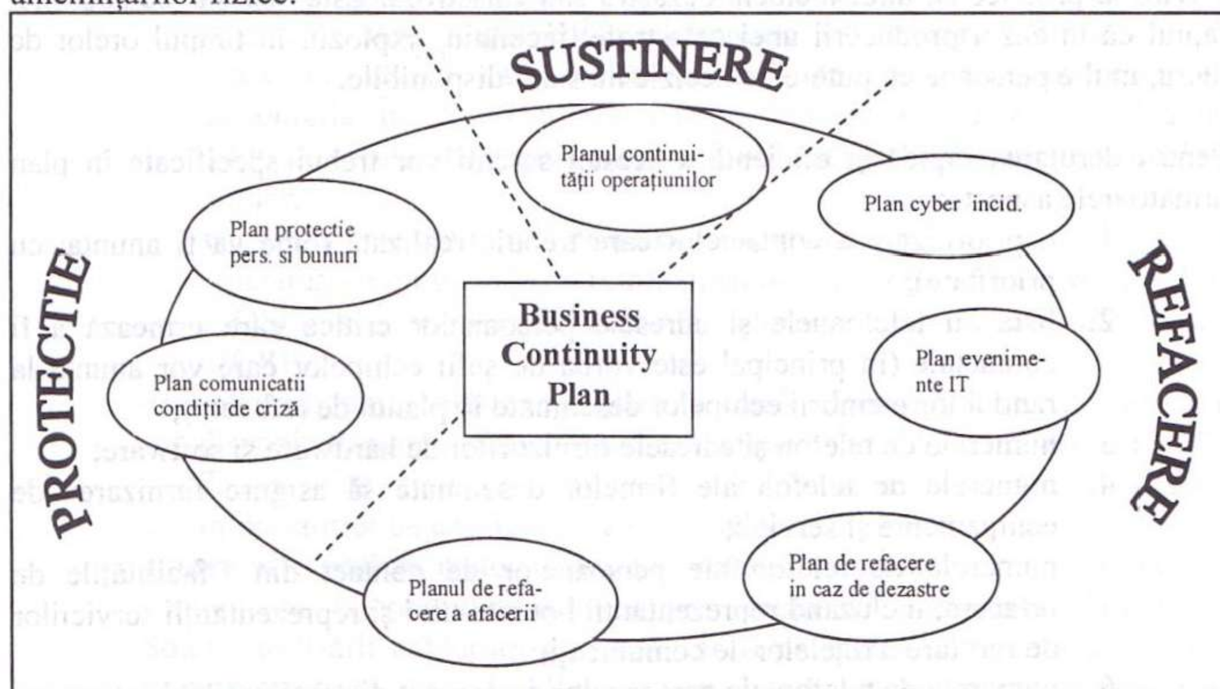


Figura 7.4.1 **Componentele BCP**

Pentru realizarea fazelor de planificare, implementare şi evaluare a BCP se impune soluţionarea următoarele aspecte:

1. politicile care vor guverna eforturile de continuare a afacerii şi de refacere;
2. scopurile/echipamentele/produsele pentru fiecare fază;
3. facilităţi alternative pentru executarea task-urilor şi operaţiilor;
4. resursele de informaţii critice ce trebuie asigurate (date şi sisteme);
5. persoanele responsabile pentru completare;
6. resursele necesare pentru realizare;
7. programarea activităţilor cu stabilirea priorităţilor.

Copii ale planului trebuie păstrate în afara centrului operaţional (în locaţia facilităţii de recovery, centrul de back-up sau la domiciliul persoanelor de decizie cheie). Componentele acestui plan cuprind: lista persoanelor de decizie cheie, lista furnizorilor, copii ale poliţelor de asigurare etc.

Personalul de decizie-cheie

Planul trebuie să cuprindă o listă a persoanelor de decizie SI şi utilizatorii desemnaţi să iniţieze şi realizeze eforturile de refacere. Cerinţele de bună practică impun desemnarea unei persoane care, în baza acestei liste, va avea sarcina notificării cu privire la producerea unui incident/dezastru sau catastrofă. Este necesar de subliniat faptul că în cazul producerii unei catastrofe, incendiu, explozii, în timpul orelor de lucru, multe persoane cu putere de decizie nu sunt disponibile.

Pentru derularea rapidă şi eficientă a acestei sarcini vor trebui specificate în plan următoarele aspecte:

1. o prioritizare a contactelor care trebuie realizate (cine va fi anunţat cu prioritate);
2. lista cu telefoanele şi adresele persoanelor critice care urmează a fi contactate (în principal este vorba de şefii echipelor care vor anunţa la rândul lor membrii echipelor desemnate în planul de refacere);
3. numerele de telefon şi adresele furnizorilor de hardware şi software;
4. numerele de telefon ale firmelor desemnate să asigure furnizarea de echipamente şi servicii;
5. numerele de telefon ale persoanelor de contact din facilităţile de refacere, incluzând reprezentanţii hot site-ului şi reprezentanţii serviciilor de rerutare a reţelelor de comunicaţii;
6. numerele de telefon ale persoanelor de contact din facilităţile de stocare a copiilor de siguranţă;
7. numerele de telefon ale societăţilor de asigurare;
8. numerele de telefon ale persoanelor de contact ale serviciilor de personal;

9. numerele de telefon și persoanele de contact din agenții guvernamentale, de reglementare și judiciare.

Metode de refacere a rețelelor de telecomunicații

BCP trebuie să cuprindă prevederi speciale pentru refacerea căilor de comunicații în caz de dezastru. Rețeaua de telecomunicații este expusă acelorași riscuri ca și centrele destinate procesării datelor, dar poate fi afectată și de evenimente specifice ei cum ar fi: distrugerea centrelor de comutare (*central switching office disasters*), tăierea cablurilor, erori la nivelul software-ului de comunicații, breșe de securitate legate de hackeri (*phreakers*), alte erori umane.

Prin BCP, organizația trebuie să asigure un back-up al rețelei de comunicații care să ofere: circuite telefonice vocale, rețele pe arii extinse care să asigure conexiuni cu centrele de date distribuite, rețele locale pentru conectarea PC-urilor, furnizori pentru servicii de schimb electronic de date.

Totodată, este necesar să se stabilească pentru fiecare facilitate de comunicații cerințele critice de capacitate determinate pentru intervale diferite: două ore, opt ore, 24 de ore.
Conform CISA, pot fi utilizate următoarele metode de protejare a rețelei:

1. **redundanță** – poate fi asigurată prin mai multe soluții:
   - asigurarea unei capacități suplimentare și utilizarea surplusului de capacitate atunci când calea primară de transmisie nu mai este disponibilă. În cazul unui LAN se recomandă instalarea unui al doilea cablu pe o rută alternativă care va fi utilizat în cazul distrugerii cablului primar;
   - asigurarea mai multor căi de acces între rutere;
   - utilizarea de protocoale de rutare dinamice (ex. *Open Shortest Path First* – OSPF și respectiv *Enhanced Interior Gateway Routing Protocol* – EIGRP);
   - salvarea configurațiilor în fișiere ce vor fi utilizate în cazul afectării unor dispozitive cum ar fi *switch-uri* sau *routere*. În acest scop se poate utiliza *Trivial File Transport Protocol (TFTP)* necesar salvării și regăsirii informațiilor de configurare a dispozitivelor din rețea.
2. **rutare alternativă**: metoda constă în rutarea informației printr-un mediu de comunicație alternativ reprezentat prin cablu de cupru sau fibră optică. Soluția utilizării cablurilor cu fibră optică presupune crearea a două inele, protejate separat unul de altul, în care informația circulă în două direcții diferite și care se conectează într-un switch central. Alte soluții pot fi

reprezentate de circuite dial-up, circuite alternative dedicate, telefoane celulare şi comunicaţii prin microunde;
3. **rutare diversă** care presupune rutarea traficului prin cablări duplicat;
4. **voice recovery** – destinată organizaţiilor din domeniul finaciar şi industriilor de retail, unde comunicarea vocală este preponderentă. Presupune cablarea duplicat şi VoIP.

7.5. Particularităţi ale asigurărilor sistemelor informatice

BCP trebuie să conţină informaţii precise legate de poliţele de asigurare încheiate pentru sistemele informatice. Vom prezenta principalele tipuri de riscuri pentru care se încheie poliţe de asigurare, precizând faptul că auditorii sistemelor informatice au obligaţia de a verifica existenţa şi valabilitatea poliţelor, precum şi a evalua măsura în care acestea acoperă adecvat riscurile la care este expus sistemul informatic al organizaţiei.

Tipuri de clauze specifice poliţelor de asigurare a sistemelor informatice[4]:
- **facilităţi şi echipament** - asigură despăgubiri în cazul distrugerii facilităţilor de procesare, inclusiv a echipamentelor. Auditorul va trebui să verifice existenţa în clauza poliţei de asigurare a obligaţiei înlocuirii echipamentelor distruse cu echipamente similare ale aceluiaşi furnizor şi nu înscrierea unor formulări generice de tipul „ echipamente de acelaşi fel şi calitate";
- **refacerea mediilor de stocare (software)** acoperă riscul distrugerii mediilor de stocare a software-ului, indiferent de locaţia în care acestea se aflau (în sediul central, în afara acestuia - locaţii de păstrare a back-up-ului sau în tranzit). Despăgubirea va trebui să acopere costul refacerii software-ului şi costul mediilor de stocare, cheltuielile de back-up;
- **cheltuieli suplimentare** – sunt acoperite costurile necesare continuării operării după distrugerea facilităţilor de procesare, în speţă costul facilităţilor de back-up precum şi acoperirea pierderilor cauzate de suspendarea operaţiilor;
- **întreruperea businessului** – acoperă pierderile cauzate de întreruperea activităţii firmei ca urmare a funcţionării defectuoase a sistemelor informatice;
- **documente şi înregistrări importante** – poliţa acoperă pierderile cauzate de distrugerea unor documente de valoare sau înregistrări (altele decât cele din mediile de stocare);
- **erori şi omisiuni** – acoperă pierderile înregistrate de clienţi cauzate de erorile sau omisiunile profesioniştilor din organizaţie (analişti de sistem, proiectanţi de software, programatori, consultanţi etc.);
- **clauza de fidelitate** acoperă riscul unor acţiuni frauduloase. Pentru instituţiile financiare este specifică asigurarea de tip *commercial blanket bond;*

[4] Conform CISA.

- **transportul mediilor de stocare** – poliţa acoperă riscul pierderii sau distrugerii mediilor de stocare în timpul transportului în afara sediului.

7.6. Testarea planului

Scopul testării este de a verifica funcţionalitatea planului şi identificarea acelor componente care trebuie îmbunătăţite. Testele se recomandă a fi efectuate în weekend deoarece este esenţial să nu fie afectată activitatea curentă, iar membrii echipelor să fie disponibili.

Conform CISA, testele trebuie să îndeplinească următoarele cerinţe:

- verificarea completitudinii şi preciziei planului;
- evaluarea personalului cu atribuţii în cadrul planului;
- evaluarea nivelului de instruire a membrilor echipelor;
- evaluarea coordonării între membrii echipei BCP şi furnizorii externi;
- măsurarea capacităţii centrului de back-up de a realiza procesarea;
- evaluarea capacităţii de regăsire a înregistrărilor vitale;
- evaluarea stării şi calităţii echipamentului şi furnizorilor relocate în site-ul de refacere;
- măsurarea performanţei de ansamblu a activităţilor de procesare şi operaţionale legate de menţinerea activităţii organizaţiei.

Testarea BCP urmează trei faze, şi anume:

- **pretestul**, etapă în care se procedează de la instalarea mobilierului până la echipamente destinate comunicaţiilor telefonice. Această etapă testează capabilitatea de a pregăti locaţia de recovery în condiţiile în care evenimentul distructiv se produce fără a exista o avertizare prealabilă şi deci nici posibilitatea de a iniţia acţiuni pregătitoare;
- **testul,** etapă constând în testarea efectivă a planului urmărindu-se verificarea obiectivelor specifice BCP. Vor fi efectuate procedurile de deplasare a personalului şi echipamentelor în noua locaţie, operaţionalizarea comunicaţiilor telefonice, introducerea datelor, procesarea, contactarea şi mobilizarea furnizorilor. Persoanele abilitate vor proceda la evaluarea modului în care s-a reuşit realizarea sarcinilor stabilite prin BCP;
- **posttestul** are ca scop testarea capacităţii de delocalizare a echipamentului, personalului şi proceselor de prelucrare din centrul de recovery în locaţia operaţională iniţială. Se procedează la deconectarea şi transportul echipamentelor, ştergerea datelor de pe sistemele furnizorului de facilităţi de procesare, dealocarea personalului.

În afara etapelor sus-menţionate se poate opta pentru derularea unor teste suplimentare reprezentate de:

- **testul de pregătire** (*preparedness test*) are drept scop să evalueze anumite aspecte ale planului şi să ofere sugestii de îmbunătăţire a acestuia;
- **testul operaţional complet** presupune simularea producerii unui dezastru, şi nu doar o întrerupere a serviciilor. În acest caz, după verificarea atentă a planului în forma sa scrisă, se trece la întreruperea totală a activităţii.

Evaluarea rezultatelor testelor

Fiecare etapă a testelor trebuie documentată pentru a se putea estima gradul de reuşită. Se recomandă ca fiecare echipă să întocmească un jurnal în care să consemneze principalele sarcini efectuate şi problemele intervenite, aceste informaţii devenind în condiţii reale de criză o sursă de informaţii extrem de utilă.

Evaluarea modului de realizare a sarcinilor se poate face prin determinarea următorilor parametrii:

- **timpul** necesar realizării sarcinilor.
- **volumul** de muncă depus în centrul de back-up de către echipa de funcţionari şi personalul de procesare operaţională.
- **numărul** de echipamente transportate şi operaţionalizate faţă de cel cerut, numărul de documente vitale aduse în locaţia de back-up faţă de cel prevăzut în plan, numărul sistemelor critice refăcute.
- **acurateţea** înregistrărilor introduse şi procesate în centrul de recovery, comparativ cu cea realizată în mod normal (exprimată procentual). Acurateţea prelucrărilor este estimată prin compararea rezultatelor procesării în centrul de recovery cu cele rezultate prin procesarea în condiţii normale.

Actualizarea planurilor

Sistemele informatice se caracterizează printr-o dezvoltare şi adaptare continuă la noile cerinţe de business fiind afectate atât componentele hardware şi de comunicaţie, cât şi componentele software. Dinamica lor impune revizuirea periodică a BCP. Acest lucru este determinat de:

- modificările intervenite în strategia organizaţiei;

- noile componente hardware şi software achiziţionate sau realizate care pot expune sistemul la noi ameninţări;
- noi sisteme devenite critice ca urmare a modificărilor la nivelul strategiei şi proceselor afacerii.

De aceea, ori de câte ori se produc modificări semnificative în sistemul informatic, actualizarea BCP şi testarea componentelor în cauză vor trebui realizate. Recomandările de bună practică impun revizuirea şi testarea anuală a BCP, avându-se în vedere modificările inevitabile ce se produc, fie chiar numai ca urmare a înlocuirii/achiziţionării de echipamente, migrării personalului, actualizărilor software-ului. Sarcina actualizării BCP revine coordonatorului planului, acesta urmând să deruleze următoarele activităţi:

- elaborarea programului de revizuire periodică şi actualizare a BCP, fiind solicitate toate persoanele cu atribuţii pe linia planului de refacere, în sensul elaborării de revizuiri şi formulării de propuneri/comentarii;
- actualizarea planului (în termen de 30 de zile de la primirea tuturor revizuirilor din partea persoanelor solicitate în acest sens);
- iniţierea de revizuiri neplanificate în cazul realizării unor modificări semnificative;
- pregătirea şi coordonarea testelor planificate şi evaluarea rezultatelor testelor;
- planificarea activităţilor de instruire a personalului stabilit pentru proceduri de urgenţă şi refacere. Şedinţele de pregătire vor trebui planificate în termen de 30 de zile de la data actualizării planurilor;
- realizarea evidenţei modificărilor, testărilor şi instruirilor legate de BCP;
- actualizarea, cel puţin trimestrial, a listei personalului şi datelor de contact, precum şi a modificărilor în statusul şi responsabilităţile persoanelor în cadrul organizaţiei.

Back-up şi proceduri de refacere

Refacerea în cazul producerii unui eveniment (ce poate fi reprezentat chiar de o eroare operaţională sau hardware) care a generat afectări sau chiar distrugeri parţiale sau totale ale bazei de date presupune utilizarea unor copii de siguranţă. Copiile de siguranţă (backup-ul) se realizează atât pentru date, cât şi pentru software (de bază şi aplicaţii). Frecvenţa realizării copiilor este direct proporţională cu volumul tranzacţiilor şi importanţa datelor pentru organizaţie şi este stabilită prin procedura specifică. În aceeaşi procedură se precizează tipul copiilor, parţiale sau totale, şi momentele de timp când trebuie realizat fiecare tip de copie.

Cea mai populară tehnică de back-up este GFS (bunic-tată-fiu) care presupune următoarea desfăşurare:

- se fac copii zilnice (parţiale sau totale aşa cum se precizează în procedura de back-up);
- copia ultimei zile din săptămână devine copia săptămânii (tată);
- copiile zilnice ale săptămânii anterioare pot fi rescrise în săptămâna următoare, mai puţin cea a ultimei zile, devenită copia săptămânii;
- la sfârşitul lunii, ultima copie realizată (copia ultimei săptămâni) devine copia lunii (bunic);
- copiile săptămânilor, mai puţin copia lunii, pot fi refolosite;
- copia ultimei luni din an devine copia anului;
- copiile lunilor, precum şi copia anului se păstrează în locaţia rezervată păstrării copiilor de siguranţă şi nu se vor rescrie.

În cadrul organizaţiei trebuie să existe o politică de back-up pentru fiecare sistem sau grup de sisteme care trebuie să prevadă:

- când şi cum (parţial sau total) se realizează copiile, unde se păstrează aceste copii şi pentru cât timp?
- frecvenţa realizării copiilor şi cine este responsabil pentru verificarea corectitudinii lor;
- numele sub care se salvează fişierul copie realizat şi modul de etichetare a benzii sau cartuşului cuprinzând copia realizată;
- cum se realizează evidenţa copiilor în arhivă şi cum pot fi recuperate copiile din arhivă (persoane autorizate să depună/ridice copii, înregistrarea datei depunerii/ridicării copiilor, data returnării copiilor la arhivă şi persoana care a făcut ridicarea/returnarea copiilor etc.).

Copiile fişierelor-master trebuie realizate la sfârşitul procedurilor de actualizare pentru a se menţine sincronizarea dintre fişiere şi sisteme. Fişierele de tranzacţii trebuie să coincidă cu fişierele-master, astfel încât o versiune anterioară a fişierului-master să poată fi actualizată utilizând copiile fişierelor de tranzacţii. Fişierele create în timp real necesită tehnici speciale de back-up: duplicarea jurnalelor tranzacţiilor, eşantionarea timpului tranzacţiilor, simularea comunicaţiei. Copiile sistemelor de gestiune a bazelor de date se realizează utilizând facilităţi oferite de însuşi SGBD.

Copiile software-ului privesc atât sistemele de operare, limbajele de programare, compilatoarele, utilitarele și aplicațiile. În cazul aplicațiilor se realizează copii atât pentru fișierele-sursă, cât și fișierele-obiect.

În egală măsură, în cadrul organizației trebuie să existe o politică de restaurare, care va trebui să cuprindă:

- persoana responsabilă cu verificarea operării corecte;
- o descriere detaliată a modului de restaurare a datelor pentru toate aplicațiile;
- în mod distinct, o descriere detaliată a modului de restaurare a sistemului de operare;
- momentele realizării restaurărilor în cazul diferitelor scenarii de dezastre;
- obligativitatea testării anuale a politicii de restore.

Menționăm necesitatea efectuării periodice (minimum o dată pe an) de teste privind procedura de restaurare pentru a se verifica măsura în care aceasta este corect elaborată, este cunoscută de persoanele autorizate să o realizeze, datele din fișierele-copii sunt acoperitoare pentru refacerea fișierelor operaționale.

O atenție deosebită se acordă caracteristicilor ce trebuie îndeplinite de locația stabilită pentru păstrarea copiilor de siguranță. Aceste caracteristici vizează asigurarea unui mediu optim din punct de vedere al temperaturii, ventilației, umidității, protecției la unde electromagnetice, protecție la incendiu. Este recomandată depunerea copiilor în dulapuri speciale, asigurând protecție la incendiu. Menționăm că și transportul copiilor de siguranță de la locația în care s-au realizat în locația stabilită pentru librărie se va realiza în genți speciale, securizate.

Locația selectată pentru librăria copiilor de siguranță trebuie să prezinte mijloace de securizare și control al accesului (uși securizate, camere de luat vederi), trebuie să fie plasată la un nivel adecvat în cadrul imobilului (plasarea la subsolul unui imobil nefiind recomandată), un altul decât cel al locației de procesare a datelor, nu trebuie să prezinte ferestre și nu trebuie să poată fi localizată din exterior. Numai persoanele autorizate vor trebui să aibă acces la aceste copii, iar persoana însărcinată cu administrarea librăriei va trebui să realizeze o evidență foarte strictă cu privire la depunerile de copii (ce copie s-a depus, de cine, când) precum și la ridicarea copiilor și momentul returnării acestora.

În locaţia rezervată păstrării copiilor de siguranţă se vor păstra şi copii ale documentaţiilor (ghiduri de operare, manuale-utilizator), cât şi documente importante pentru organizaţie precum şi copia BCP. În cele ce urmează vom prezenta succint documentaţia păstrată în locaţia rezervată copiilor de siguranţă:

- proceduri de operare (manuale ale aplicaţiilor, manuale pentru operarea sistemelor, proceduri speciale);
- documentaţia sistemelor şi programelor cuprinzând organigrame, programe sursă listate, descrierea programelor, manuale-utilizator;
- proceduri speciale (reprezentate de alte proceduri decât cele ordinare, cum ar fi proceduri de procesare în condiţii de urgenţă);
- documente primare şi rapoarte (copii ale unor documente importante pentru organizaţie inclusiv copii ale poliţelor de asigurare, microfilme cu rapoarte sau sinteze necesare auditului etc.);
- copia BCP.

7.7. Auditul planului de refacere şi continuare a afacerii

Datorită importanţei sale pentru organizaţie, BCP este supus evaluării de către auditorul sistemului informatic. Regulile de bună practică recomandă ca obiectivele acestei misiuni să fie reprezentate de :

- înţelegerea şi evaluarea strategiei de continuare a activităţii şi a conexiunilor acesteia cu obiectivele de business;
- evaluarea adecvării şi acurateţei BCP;
- evaluarea eficienţei BCP în baza testelor anterioare realizate de personalul IT şi utilizatori finali;
- inspectarea locaţiilor destinate stocării back-up-urilor în scopul evaluării adecvării acestora din punct de vedere al controalelor de securitate şi ale mediului. Verificarea conţinutului şi periodicităţii copiilor de siguranţă;
- evaluarea capacităţii sistemului informatic şi al personalului de a răspunde în condiţii de urgenţă. În acest scop se procedează la evaluarea procedurilor elaborate, verificarea documentelor privind instruirile derulate în cadrul organizaţiei şi a rezultatelor testelor efectuate;
- evaluarea activităţii de revizure şi actualizare a BCP;
- verificarea măsurii în care procedurile şi planul de refacere sunt scrise clar, sunt uşor de înţeles. Acest lucru poate fi determinat prin evaluarea acestor proceduri, desfăşurarea de interviuri cu personalul implicat în aplicarea planului pentru a se vedea măsura în care acesta îşi cunoaşte rolul şi stăpâneşte procedurile pe care trebuie să le execute.

Pentru a proceda la revizuirea BCP, auditorii trebuie să dispună de o copie actualizată a planului. În baza informațiilor dobândite, auditorul trebuie să verifice următoarele aspecte:

- realizarea actualizării copiilor planului;
- evaluarea eficienței procedurilor;
- evaluarea modului în care s-a procedat la identificarea, prioritizarea și susținerea aplicațiilor critice;
- verificarea măsurii în care pentru toate aplicațiile s-a determinat nivelul de toleranță în cazul producerii unui eveniment distructiv;
- verificarea instalării în site-ul de refacere (de tip hot site) a versiunii corecte de software și a compatibilității diferitelor componente software;
- verificarea adecvării și completitudinii listelor cuprinzând persoanele cu atribuții în BCP, a furnizorilor, contactelor din hotsite. Verificarea prin sondaj a valabilității telefoanelor și adreselor persoanelor înscrise în lista contactelor și a măsurii în care acestea dispun de copii actualizate ale planului;
- evaluarea procedurilor de documentare a testelor;
- evaluarea procedurilor de actualizare a planului.

În completarea sarcinilor sus-menționate putem adăuga:

- evaluarea tuturor procedurilor scrise din punct de vedere al adecvării, acurateței, ținerii la zi și ușurinței de a fi înțelese;
- identificarea necesității ca tranzacțiile reintroduse prin procesul de recovery să fie identificate în mod separat de tranzacțiile introduse în condiții normale;
- evaluarea măsurii în care planul prevede în mod adecvat procedurile din centrul de recovery;
- determinarea măsurii în care echipele de recovery dispun de proceduri scrise.

Auditorul va proceda la evaluarea rezultatelor testelor pentru a vedea dacă s-a procedat la luarea măsurilor necesare corectării erorilor/problemelor identificate. Auditorul trebuie să verifice în egală măsură adecvarea testelor efectuate și a măsurilor dispuse în urma lor.

Auditorul va proceda la verificarea locațiilor rezervate păstrării copiilor de siguranță pentru a vedea modul în care acestea răspund cerințelor privitoare la asigurarea mediului adecvat de păstrare, protecției față de accesul neautorizat, adecvării și completitudinii copiilor, precum și a modului lor de gestiune. Se va proceda la un

inventar al copiilor (atât pentru fişierele de date, cât şi cele ale software-ului) pentru a se vedea completitudinea şi actualitatea acestora, corecta etichetare a volumelor şi organizarea librăriei. Se va proceda totodată la inspectarea şi evaluarea facilităţii de procesare alternativă pentru a vedea mijloacele de protecţie existente (detectoare de fum şi respectiv apă, mijloace de măsurare a umidităţii şi temperaturii), existenţa surselor de asigurare a furnizării neîntrerupte a energiei electrice (echipamente UPS), controlul accesului. Se va proceda la inspectarea echipamentului existent şi a adecvării acestuia în raport cu nevoile de procesare.

Auditorul va intervieva personalul-cheie pentru reuşita BCP, pentru a vedea măsura în care acesta cunoaşte şi înţelege responsabilităţile care i-au fost atribuite, este instruit periodic, cunoaşte ultima versiune a planului.

În egală măsură, auditorul va proceda la evaluarea clauzelor contractelor încheiate cu furnizorii de facilităţi de procesare alternativă, precum şi a poliţelor de asigurare pentru ca acestea să conţină clauze clare şi acoperitoare pentru riscurile potenţiale.

7.8. Test de evaluare a cunoştinţelor

1. Primul scop pentru implementarea unui sistem redundant de discuri RAID (*Redundent Array of Inexpensive Disks*) nivel 1 pe un server de fişiere este:
   a. îmbunătăţirea performanţelor de arhivare;
   b. furnizarea autenticităţii utilizatorului;
   c. asigurarea disponibilităţii datelor;
   d. asigurarea confidenţialităţii datelor.

2. O facilitate externă de procesare a informaţiei:
   a. ar trebui să aibă aceeaşi restricţie la accesul fizic ca şi prima locaţie de procesare;
   b. ar trebui identificată mai uşor din afară pentru ca, în caz de urgenţă, să fie uşor de găsit;
   c. ar trebui să fie localizată în apropierea locaţiei iniţiale, pentru a fi operaţională cât mai repede;
   d. nu trebuie să aibă acelaşi nivel de monitorizare a mediului ca şi locaţia iniţială.

3. Care dintre următoarele afirmaţii este cea mai importantă pentru a furniza un plan de recuperare în caz de dezastre?

a. copii de siguranță ale programelor-obiect compilate;
b. acord privind procesarea reciprocă;
c. lista numerelor de telefon pentru persoanele de contact;
d. furnizarea formularelor speciale.

4. Care dintre următoarele componente ale planului de recuperare/continuitate în caz de dezastre furnizează cea mai mare asigurare de recuperare după dezastru?
a. facilitatea alternativă va fi disponibilă până când facilitatea de procesare a informației inițială este restabilită;
b. managementul utilizatorilor este implicat în identificarea sistemelor critice și în timpul de recuperare a acestora;
c. copiile planului de recuperare sunt ținute la domiciliul unuia dintre angajații importanți în luarea deciziilor;
d. asigurarea conducerii că planurile de continuitate a afacerii pot fi puse în aplicare și că procedurile sunt cele adecvate.

5. Primul obiectiv al planului de recuperare și continuare a afacerii în caz de dezastru trebuie să fie:
a. salvarea elementelor critice ale SI;
b. asigurarea continuității operațiilor;
c. minimizarea pierderilor societății;
d. protecția vieții oamenilor.

6. Care dintre următoarele afirmații este cea mai mare preocupare, când facilitățile de back-up ale organizației sunt la o locație „caldă"?
a. disponibilitatea hardware;
b. disponibilitatea la căldură – umiditate și aer condiționat a echipamentului;
c. conexiunea la curentul electric adecvată;
d. existența unei rețele de telecomunicații.

7. Propunerea primă pentru analiza impactului afacerii (BIA) este:
a. furnizarea unui plan pentru reluarea operațiilor după dezastru;
b. identificarea evenimentelor care au un impact în continuitatea operațiilor organizației;

c. publicitatea angajamentelor organizației privind securitatea fizică şi logică;

d. furnizarea unui cadru de lucru pentru un plan efectiv de recuperare în caz de dezastre (DRP).

8. După implementarea unui DRP, costul operațiilor pre- şi postdezastru pentru o organizație va:

a. avea o pondere de scădere;

b. rămâne acelaşi;

c. creşte;

d. creşte sau va scădea, depinzând de natura afacerii.

9. Un plan de recuperare în caz de dezastru pentru o afacere ar trebui să recupereze mai întâi:

a. toate informațiile procesate de sistem;

b. toate aplicațiile de procesare financiară;

c. doar acele aplicații proiectate de conducerea SI;

d. procesarea în ordin prioritar este definită de conducătorul afacerii.

10. În timpul evaluării planului de continuitate a afacerii, auditorul va verifica dacă datele şi fişierele sunt salvate în mod periodic. Ce caracteristică a planului demonstrează aceasta?

a. flexibilitatea;

b. completitudinea;

c. recuperarea;

d. răspunderea.